JO3P0958 YS01

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　８月　７日

出願番号
Application Number: 特願２００２－２３０２７０

[ST.10/C]: [ＪＰ２００２－２３０２７０]

出願人
Applicant(s): ソニー株式会社

２００３年　５月２７日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０３９６３８

【書類名】　特許願
【整理番号】　0290478502
【提出日】　平成14年 8月 7日
【あて先】　特許庁長官殿
【国際特許分類】　G09C 1/00
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　金丸　昌司
【特許出願人】
【識別番号】　000002185
【氏名又は名称】　ソニー株式会社
【代理人】
【識別番号】　100093241
【弁理士】
【氏名又は名称】　宮田　正昭
【電話番号】　03-5541-7577
【選任した代理人】
【識別番号】　100101801
【弁理士】
【氏名又は名称】　山田　英治
【電話番号】　03-5541-7577
【選任した代理人】
【識別番号】　100086531
【弁理士】
【氏名又は名称】　澤田　俊夫
【電話番号】　03-5541-7577
【手数料の表示】
【予納台帳番号】　048747

【納付金額】　　21,000円

【提出物件の目録】

【物件名】　　明細書　1

【物件名】　　図面　1

【物件名】　　要約書　1

【包括委任状番号】　9904833

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　暗号強度指標算出方法、およびコンピュータ・プログラム

【特許請求の範囲】

【請求項１】

暗号処理アルゴリズムの暗号強度指標算出方法であり、

線形変換部と非線形変換部から成る鍵スケジュール部を有し、前記鍵スケジュール部の初期値がU_i，（ｉ＝１，２，．．．）、中間値が$Z_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝０，１，２，．．．）、非線形変換部出力が$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）、前記中間値Z_i，（ｉ＝１，２，．．．）、より生成されるラウンド鍵が$K_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）と表され、

マスター鍵から初期値U_i，（ｉ＝１，２，．．．）、を生成するステップと、初期値U_i，（ｉ＝１，２，．．．）、から中間値$Z_i^{(0)}$，（ｉ＝１，２，．．．）を計算するステップと、中間値$Z_i^{(r-1)}$，（ｉ＝１，２，．．．）から中間値$Z_i^{(r)}$，（ｉ＝１，２，．．．）を計算する複数のステップと、前記中間値$Z_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）、及び初期値U_i，（ｉ＝１，２，．．．）から非線形変換部出力$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）を計算するステップと、前記中間値$Z_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）及び前記非線形変換部出力$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）からラウンド鍵$K_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）を計算するステップとを有する共通鍵ブロック暗号処理アルゴリズムを暗号強度指標算出対象の暗号処理アルゴリズムとして設定するステップと、

前記ラウンド鍵$K_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）が前記初期値U_i，（ｉ＝１，２，．．．）及び前記非線形変換部出力$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）の線形結合で表記できるように前記中間値$Z_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）変数を消去するステップと、

前記線形結合式を、右辺が前記初期値U_i，（ｉ＝１，２，．．．）及び前記

非線形変換部出力$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）の項のみを有するように移項した連立線形方程式に変換するステップと、

前記連立線形方程式を行列方程式に変換するステップと、

前記行列方程式の両辺に、右辺の行列を階段行列に変形する行変形ユニタリ行列を左から乗じるステップと、

前記階段行列の行数から前記階段行列のｒａｎｋ値を減じた数をＮとしたとき、変換後の前記行列方程式の左辺の行列の下Ｎ行からなる新たな行列を生成するステップと、

前記ラウンド鍵$K_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）を要素とする列ベクトルを前記生成された新たな行列に乗ずることによってＮ個の線形関係式を求めるステップと、

を有することを特徴とする暗号強度指標算出方法。

【請求項２】

暗号処理アルゴリズムの暗号強度指標算出処理実行プログラムを記述したコンピュータ・プログラムであり、

線形変換部と非線形変換部から成る鍵スケジュール部を有し、前記鍵スケジュール部の初期値がU_i，（ｉ＝１，２，．．．）、中間値が$Z_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝０，１，２，．．．）、非線形変換部出力が$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）、前記中間値Z_i，（ｉ＝１，２，．．．）、より生成されるラウンド鍵が$K_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）と表され、

マスター鍵から初期値U_i，（ｉ＝１，２，．．．）、を生成するステップと、初期値U_i，（ｉ＝１，２，．．．）、から中間値$Z_i^{(0)}$，（ｉ＝１，２，．．．）を計算するステップと、中間値$Z_i^{(r-1)}$，（ｉ＝１，２，．．．）から中間値$Z_i^{(r)}$，（ｉ＝１，２，．．．）を計算する複数のステップと、前記中間値$Z_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）、及び初期値U_i，（ｉ＝１，２，．．．）から非線形変換部出力$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）を計算するステップと、前記中間値$Z_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）及び前記非線形変換部出力$V_i^{(r)}$，（ｉ＝１，２，

．．．，ｒ＝１，２，．．．）からラウンド鍵$K_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）を計算するステップとを有する共通鍵ブロック暗号処理アルゴリズムを暗号強度指標算出対象の暗号処理アルゴリズムとして設定するステップと、

前記ラウンド鍵$K_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）が前記初期値U_i，（ｉ＝１，２，．．．）及び前記非線形変換部出力$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）の線形結合で表記できるように前記中間値$Z_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）変数を消去するステップと、

前記線形結合式を、右辺が前記初期値U_i，（ｉ＝１，２，．．．）及び前記非線形変換部出力$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）の項のみを有するように移項した連立線形方程式に変換するステップと、

前記連立線形方程式を行列方程式に変換するステップと、

前記行列方程式の両辺に、右辺の行列を階段行列に変形する行変形ユニタリ行列を左から乗じるステップと、

前記階段行列の行数から前記階段行列のｒａｎｋ値を減じた数をＮとしたとき、変換後の前記行列方程式の左辺の行列の下Ｎ行からなる新たな行列を生成するステップと、

前記ラウンド鍵$K_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）を要素とする列ベクトルを前記生成された新たな行列に乗ずることによってＮ個の線形関係式を求めるステップと、

を有することを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、暗号強度指標算出方法、およびコンピュータ・プログラムに関する。さらに、詳細には、共通鍵ブロック暗号の安全性・強度を評価するための指標を算出する暗号強度指標算出方法、およびコンピュータ・プログラムに関する。

【０００２】

【従来の技術】

暗号処理アルゴリズムには様々なものがあるが、大きく分類すると、暗号化鍵と復号化鍵を異なる鍵、例えば公開鍵と秘密鍵として設定する公開鍵暗号方式と、暗号化鍵と復号化鍵を共通の鍵として設定する共通鍵暗号方式とに分類される。

【０００３】

共通鍵暗号方式にも様々なアルゴリズムがあるが、その１つに共通鍵をベースとして複数の鍵を生成して、生成した複数の鍵を用いて暗号処理を実行する方式がある。複数の鍵の生成方式としてラウンド関数を用いる方式がある。これは、共通鍵に対してラウンド関数を作用させ、その出力値をもとに新たな鍵を生成し、さらに出力値にラウンド関数を作用させて得られる次の出力値をもとに次の鍵を生成するといった手順を繰り返して実行することによって複数の鍵を生成する方式である。このような鍵生成方式を適用したアルゴリズムの代表的なものが共通鍵ブロック暗号方式である。

【０００４】

共通鍵ブロック暗号のアルゴリズムは、主として、ラウンド関数部と鍵スケジュール部とに分けることができる。従来、共通鍵ブロック暗号を設計する際には、鍵関連攻撃等に対する安全性を確保するため、暗号の設計者は、ラウンド鍵間の単純な関係式が成立しないように、注意深く鍵スケジュール部の設計を行うことが要請されてきた。

【０００５】

このような指針に基づいて設計された暗号として、東芝が提案した共通鍵ブロック暗号「Hierocrypt」がある。Hierocryptについては、例えば「"The Block Cipher Hierocrypt ", K.Ohkuma,et al Selected areas in cryptography, LNCS 2012,pp.72-88,2000.」を参照されたい。Hierocryptの鍵スケジュール部は、Feistel構造と呼ばれる繰り返し構造をもっているが、Feistel構造の右半分の線形変換部に、ラウンド依存定数をXOR加算することによって鍵関連攻撃を回避することを試みている。

【０００６】

ところが、実際にはHierocryptの作者が予期していなかったラウンド鍵間の線形関係式が成立することが、２００１年にFuruya等によって発見された。詳細については、例えば、「S. Furuya and V. Rijmen, Observations on Hierocrypt-3/L1 Key-scheduling Algorithms, Second NESSIE workshop, 2001.」に述べられている。

【０００７】

【発明が解決しようとする課題】

しかし、上述のFuruya等によって行われた手法は、Hierocryptの鍵スケジュール部のアルゴリズムを試行錯誤で組み合わせることによってラウンド鍵間の線形関係式を導出するものであるため、発見された関係式が全てを網羅しているという保証はなかった。更に、試行錯誤的な方法では、鍵スケジュールが一層複雑になった場合、関係式を求めるのは困難を極める。

【０００８】

本発明は、鍵スケジュールの複雑性に拘わらず、共通鍵ブロック暗号方式におけるラウンド鍵間の線形関係式をすべて網羅することを可能としたものであり、導出される線形関係式に基づいて、共通鍵ブロック暗号方式の暗号強度評価を行なうことを可能とした暗号強度指標算出方法、およびコンピュータ・プログラムを提供することを目的とする。

【０００９】

【課題を解決するための手段】

本発明の第１の側面は、

暗号処理アルゴリズムの暗号強度指標算出方法であり、

線形変換部と非線形変換部から成る鍵スケジュール部を有し、前記鍵スケジュール部の初期値がU_i，（ｉ＝１，２，．．．）、中間値が$Z_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝０，１，２，．．．）、非線形変換部出力が$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）、前記中間値Z_i，（ｉ＝１，２，．．．）、より生成されるラウンド鍵が$K_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）と表され、

マスター鍵から初期値U_i，（ｉ＝１，２，．．．）、を生成するステップと

、初期値U_i，（ｉ＝１，２，．．．）、から中間値$Z_i^{(0)}$，（ｉ＝１，２，．．．）を計算するステップと、中間値$Z_i^{(r-1)}$，（ｉ＝１，２，．．．）から中間値$Z_i^{(r)}$，（ｉ＝１，２，．．．）を計算する複数のステップと、前記中間値$Z_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）、及び初期値U_i，（ｉ＝１，２，．．．）から非線形変換部出力$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）を計算するステップと、前記中間値$Z_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）及び前記非線形変換部出力$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）からラウンド鍵$K_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）を計算するステップとを有する共通鍵ブロック暗号処理アルゴリズムを暗号強度指標算出対象の暗号処理アルゴリズムとして設定するステップと、

前記ラウンド鍵$K_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）が前記初期値U_i，（ｉ＝１，２，．．．）及び前記非線形変換部出力$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）の線形結合で表記できるように前記中間値$Z_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）変数を消去するステップと、

前記線形結合式を、右辺が前記初期値U_i，（ｉ＝１，２，．．．）及び前記非線形変換部出力$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）の項のみを有するように移項した連立線形方程式に変換するステップと、

前記連立線形方程式を行列方程式に変換するステップと、

前記行列方程式の両辺に、右辺の行列を階段行列に変形する行変形ユニタリ行列を左から乗じるステップと、

前記階段行列の行数から前記階段行列のｒａｎｋ値を減じた数をＮとしたとき、変換後の前記行列方程式の左辺の行列の下Ｎ行からなる新たな行列を生成するステップと、

前記ラウンド鍵$K_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）を要素とする列ベクトルを前記生成された新たな行列に乗ずることによってＮ個の線形関係式を求めるステップと、

を有することを特徴とする暗号強度指標算出方法にある。

【００１０】

さらに、本発明の第２の側面は、

暗号処理アルゴリズムの暗号強度指標算出処理実行プログラムを記述したコンピュータ・プログラムであり、

線形変換部と非線形変換部から成る鍵スケジュール部を有し、前記鍵スケジュール部の初期値がU_i，（ｉ＝１，２，．．．）、中間値が$Z_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝０，１，２，．．．）、非線形変換部出力が$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）、前記中間値Z_i，（ｉ＝１，２，．．．）、より生成されるラウンド鍵が$K_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）と表され、

マスター鍵から初期値U_i，（ｉ＝１，２，．．．）、を生成するステップと、初期値U_i，（ｉ＝１，２，．．．）、から中間値$Z_i^{(0)}$，（ｉ＝１，２，．．．）を計算するステップと、中間値$Z_i^{(r-1)}$，（ｉ＝１，２，．．．）から中間値$Z_i^{(r)}$，（ｉ＝１，２，．．．）を計算する複数のステップと、前記中間値$Z_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）、及び初期値U_i，（ｉ＝１，２，．．．）から非線形変換部出力$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）を計算するステップと、前記中間値$Z_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）及び前記非線形変換部出力$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）からラウンド鍵$K_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）を計算するステップとを有する共通鍵ブロック暗号処理アルゴリズムを暗号強度指標算出対象の暗号処理アルゴリズムとして設定するステップと、

前記ラウンド鍵$K_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）が前記初期値U_i，（ｉ＝１，２，．．．）及び前記非線形変換部出力$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）の線形結合で表記できるように前記中間値$Z_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）変数を消去するステップと、

前記線形結合式を、右辺が前記初期値U_i，（ｉ＝１，２，．．．）及び前記非線形変換部出力$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）の項の

みを有するように移項した連立線形方程式に変換するステップと、

前記連立線形方程式を行列方程式に変換するステップと、

前記行列方程式の両辺に、右辺の行列を階段行列に変形する行変形ユニタリ行列を左から乗じるステップと、

前記階段行列の行数から前記階段行列のｒａｎｋ値を減じた数をＮとしたとき、変換後の前記行列方程式の左辺の行列の下Ｎ行からなる新たな行列を生成するステップと、

前記ラウンド鍵$K_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）を要素とする列ベクトルを前記生成された新たな行列に乗ずることによってＮ個の線形関係式を求めるステップと、

を有することを特徴とするコンピュータ・プログラムにある。

【００１１】

【作用】

本発明の構成によれば、鍵スケジュールの複雑性に拘わらず、共通鍵ブロック暗号方式におけるラウンド鍵間の線形関係式をすべて網羅することが可能となり、導出される線形関係式に基づいて、共通鍵ブロック暗号方式の暗号強度評価を実行することが可能となる。

【００１２】

本発明の構成によれば、暗号アルゴリズムのうち、鍵スケジュール部のアルゴリズムをベクトルと行列を用いて方程式で表現し、その行列方程式における非線形変換出力値及び初期値をユニタリ変換を利用して消去することにより、ラウンド鍵間の全ての線形関係式を求めることが可能となる。

【００１３】

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、ＣＤやＦＤ、ＭＯなどの記憶媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【００１４】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【００１５】

【発明の実施の形態】

以下、本発明の暗号強度指標算出方法について詳細に説明する。まず、本発明の暗号強度指標算出処理の手順の概略について図１の処理フローを参照して説明する。その後、複数の具体的な共通鍵ブロック暗号アルゴリズムを例として、本発明の暗号強度指標算出処理を実行した例について説明する。

【００１６】

[暗号強度指標算出処理概要]

図１は、本発明の暗号強度指標算出処理の処理手順をフローチャートとして示した図である。各処理ステップの概略について説明する。

【００１７】

まず、ステップＳ１０１では、暗号強度指標算出処理対象となる暗号アルゴリズムを設定する。ここで暗号強度指標算出処理対象となる暗号アルゴリズムは、共通鍵ブロック暗号アルゴリズムである。

【００１８】

具体的には、線形変換部と非線形変換部から成る鍵スケジュール部を有し、前記鍵スケジュール部の初期値がU_i，（ｉ＝１，２，．．．）、中間値が$Z_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝０，１，２，．．．）、非線形変換部出力が$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）、前記中間値Z_i，（ｉ＝１，２，．．．）、より生成されるラウンド鍵が$K_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）と表され、マスター鍵から初期値U_i，（ｉ＝１，２，．．．）、を生成するステップと、初期値U_i，（ｉ＝１，２，．．．）、から中間値$Z_i^{(0)}$，（ｉ＝１，２，．．．）を計算するステップと、中間値$Z_i^{(r-1)}$，（ｉ＝１，２，．．．）から中間値$Z_i^{(r)}$，（ｉ＝１，２，．．．）を計算する

複数のステップと、前記中間値$Z_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）、及び初期値U_i，（ｉ＝１，２，．．．）から非線形変換部出力$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）を計算するステップと、前記中間値$Z_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）及び前記非線形変換部出力$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）からラウンド鍵$K_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）を計算するステップとを有する共通鍵ブロック暗号処理アルゴリズムを暗号強度指標算出対象の暗号処理アルゴリズムとして設定する。

【００１９】

次に、ステップＳ１０２において、ステップＳ１０１において設定した共通鍵ブロック暗号処理アルゴリズムの中間変数を消去する。すなわち、ラウンド鍵$K_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）が前記初期値U_i，（ｉ＝１，２，．．．）及び前記非線形変換部出力$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）の線形結合で表記できるように前記中間値$Z_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）変数を消去する処理を実行する。具体的な処理例については後述する。

【００２０】

次にステップＳ１０３において、変数移項処理を実行する。すなわち、前記線形結合式を、右辺が前記初期値U_i，（ｉ＝１，２，．．．）及び前記非線形変換部出力$V_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）の項のみを有するように移項した連立線形方程式に変換する処理を実行する。具体的な処理例については後述する。

【００２１】

次に、ステップＳ１０４において、行列方程式変換処理を実行する。すなわち、前記連立線形方程式を行列方程式に変換する処理を実行する。具体的な処理例については後述する。

【００２２】

次に、ステップＳ１０５において、ユニタリ変換処理を実行する。すなわち、前記行列方程式の両辺に、右辺の行列を階段行列に変形する行変形ユニタリ行列

を左から乗じる処理を実行する。具体的な処理例については後述する。

【００２３】

次にステップＳ１０６において、小行列選択処理を実行する。すなわち、前記階段行列の行数から前記階段行列のｒａｎｋ値を減じた数をＮとしたとき、変換後の前記行列方程式の左辺の行列の下Ｎ行からなる新たな行列を生成する。具体的な処理例については後述する。

【００２４】

次にステップＳ１０７において、線形関係式生成処理を実行する。すなわち、前記ラウンド鍵$K_i^{(r)}$，（ｉ＝１，２，．．．，ｒ＝１，２，．．．）を要素とする列ベクトルを前記生成された新たな行列に乗ずることによってＮ個の線形関係式を求める。具体的な処理例については後述する。

【００２５】

上述した処理によって求められた線形関係式の数：ＮをステップＳ１０１において設定した共通鍵ブロック暗号アルゴリズムの暗号強度指標とするものである。上述した処理フローは、ステップＳ１０１において設定した共通鍵ブロック暗号アルゴリズムのラウンド鍵間の線形関係式を網羅する線形関係式の数：Ｎを求める処理として実行され、線形関係式の数：Ｎが大であるほど暗号強度が弱く、小であるほど暗号強度が強いとの判定が可能である。従って、図１に示すフローに従って求められる線形関係式数：Ｎを共通鍵ブロック暗号アルゴリズムの暗号強度指標として適用することが可能となる。

【００２６】

図１に示す処理手順に従った処理によれば、暗号アルゴリズムのうち、鍵スケジュール部のアルゴリズムをベクトルと行列を用いて方程式で表現し、その行列方程式における非線形変換出力値及び初期値をユニタリ変換を利用して消去することでラウンド鍵間の全ての線形関係式を求めることが可能となる。

【００２７】

[暗号強度指標算出処理具体例１]

次に、本発明に係る暗号強度指標算出処理具体例として、東芝から提案されたブロック暗号「Hierocrypt-L1」に対して本発明に係る暗号強度評価方法を適用

した処理例の詳細について説明する。Hierocrypt-L1は、ブロック長さ６４ｂｉｔ、鍵長１２８ｂｉｔの共通鍵ブロック暗号である。

【００２８】

まず、図１に示すステップＳ１０１の暗号処理アルゴリズムの設定ステップについて説明する。ここでは、東芝から提案されたブロック暗号「Hierocrypt-L1」の設定処理として実行する。

【００２９】

Ｏｎ，Ｉｎを各々ｎ行ｎ列の零行列、単位行列とする。これを用いて、行列Ｐ１６は以下のように定義される。

【００３０】

【数１】

$$P16 = \begin{pmatrix} I2 & O2 & I2 & O2 \\ O2 & I2 & O2 & I2 \\ O2 & I2 & I2 & I2 \\ I2 & O2 & I2 & I2 \end{pmatrix}$$

【００３１】

また、行列Ｐ１６Ｉを、行列Ｐ１６の逆行列とする。次に、行列Ｍ５、ＭＢを以下のように定義する。

【００３２】

【数２】

$$M5 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

$$MB = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

【００３３】

さらに、行列Ｍ５、ＭＢを用いて、以下のように行列Ｍ５Ｂ、ＭＢ５を定義する。

【００３４】

【数３】

$$M5B = \begin{pmatrix} M5 & O4 \\ O4 & MB \end{pmatrix}$$
$$MB5 = \begin{pmatrix} MB & O4 \\ O4 & M5 \end{pmatrix}$$

【００３５】

次に、ラウンド依存定数ベクトルＧｉ（（ｉ＝０．．．７）を以下のように定義する。

【００３６】

【数４】

Ｇ０＝(h01,h02,h03,h04,0,0,0,0)

Ｇ１＝(h11,h12,h13,h14,0,0,0,0)

Ｇ２＝(h21,h22,h23,h24,0,0,0,0)

Ｇ３＝(h31,h32,h33,h34,0,0,0,0)

Ｇ４＝(h41,h42,h43,h44,0,0,0,0)

Ｇ５＝(h41,h42,h43,h44,0,0,0,0)

Ｇ６＝(h31,h32,h33,h34,0,0,0,0)

Ｇ７＝(h21,h22,h23,h24,0,0,0,0)

【００３７】

なお、上式で用いられている定数を要素とするベクトルＨＨを、以下のように定義しておく。

【００３８】

【数５】

HH=(h01,h02,h03,h04,h11,h12,h13,h14,h21,h22,h23,h24,h31,h32,h33,h34,h41,h42,h43,h44)

【００３９】

具体的な、h01,h02,．．．,h44の値は、以下のように定義される。

【００４０】

【数６】

(h01,h01,h02,h03)=(0x5a, 0x82, 0x79, 0x99)

(h11,h11,h12,h13)=(0x6e, 0xd9, 0xeb, 0xa1)

(h21,h21,h22,h23)=(0x8f, 0x1b, 0xbc, 0xdc)

(h31,h31,h32,h33)=(0xca, 0x62, 0xc1, 0xd6)

(h41,h41,h42,h43)=(0xf7, 0xde, 0xf5, 0x8a)

【００４１】

次に、鍵スケジュール部の初期値の右半分から成るベクトルＺＺを、以下のように定義する。

【００４２】

【数７】

ZZ=(z31,z32,z33,z34,z41,z42,z43,z44)

【００４３】

これらを用いて、共通鍵暗号アルゴリズムHierocrypt-L1の鍵スケジュール部の右半分は、以下のように表せる。なお、演算子＋は、ガロア体ＧＦ（２）上の加法演算子である。

【００４４】

【数８】

Ｚ０＝Ｍ５Ｂ＊ＺＺ＋Ｇ０

Ｗ０＝Ｐ１６＊Ｚ０

Ｚ１＝Ｍ５Ｂ＊Ｗ０＋Ｇ１

Ｗ１＝Ｐ１６＊Ｚ１

Ｚ２＝Ｍ５Ｂ＊Ｗ１＋Ｇ２

Ｗ２＝Ｐ１６＊Ｚ２

Ｚ３＝Ｍ５Ｂ＊Ｗ２＋Ｇ３

Ｗ３＝Ｐ１６＊Ｚ３

Ｚ４＝Ｍ５Ｂ＊Ｗ３＋Ｇ４

Ｗ５＝ＭＢ５＊（Ｚ４＋Ｇ５）

Ｚ５＝Ｐ１６Ｉ＊Ｗ５

Ｗ６＝ＭＢ５＊（Ｚ５＋Ｇ６）

Ｚ６＝Ｐ１６Ｉ＊Ｗ６

Ｗ７＝ＭＢ５＊（Ｚ６＋Ｇ７）

Ｚ７＝Ｐ１６Ｉ＊Ｗ７

【００４５】

ここで、Z0,Z1,Z2,Z3,Z4,Z5,Z6,Z7,W0,W1,W2,W3,W5,W6,W7は、鍵スケジュール部の中間値の右半分を表す。

【００４６】

次に、これらの中間値を、下式、

【００４７】

【数９】

$Zn=Zn_3||ZN_4$

$Wn=Wn_1||WN_2$

【００４８】

のように分割して表現する。但し記号“||”は、ベクトルの連結を表す。

【００４９】

次に、各ラウンドの非線形変換部出力を、V0,V1,V2,V3,V4,V5,V6,V7とする。

但し、各々は、下記に示す４つの要素から成るベクトルである。

【００５０】

【数１０】

V0=(v01,v02,v03,v04)

V1=(v11,v12,v13,v14)

V2=(v21,v22,v23,v24)

V3=(v31,v32,v33,v34)

V4=(v41,v42,v43,v44)

V5=(v51,v52,v53,v54)

V6=(v61,v62,v63,v64)

V7=(v71,v72,v73,v74)

【００５１】

ここで、ベクトルZ_1、Z_2を下記のように設定する。

【００５２】

【数１１】

$Z_1=(z11,z12,z13,z14)$

$Z_2=(z21,z22,z23,z24)$

【００５３】

上記のように、ベクトルZ_1、Z_2を設定すると、Hierocrypt-L1の鍵スケジュール部の左半分は、以下のように表せる。

【００５４】

【数１２】

$$Z0_1=Z_2$$
$$Z0_2=Z_1+V0$$
$$Z1_1=Z0_2$$
$$Z1_2=Z0_1+V1$$
$$Z2_1=Z1_2$$
$$Z2_2=Z1_1+V2$$
$$Z3_1=Z2_2$$
$$Z3_2=Z2_1+V3$$
$$Z4_1=Z3_2$$
$$Z4_2=Z3_1+V4$$
$$Z5_1=Z4_2+V5$$
$$Z5_2=Z4_1$$
$$Z6_1=Z5_2+V6$$
$$Z6_2=Z5_1$$
$$Z7_1=Z6_2+V7$$
$$Z7_2=Z6_1$$

【００５５】

ここで、$Z0_1$，$Z0_2$，$Z1_1$，$Z1_2$，$Z2_1$，$Z2_2$，$Z3_1$，$Z3_2$，$Z4_1$，$Z4_2$，$Z5_1$，$Z5_2$，$Z6_1$，$Z6_2$，$Z7_1$，$Z7_2$は、鍵スケジュール部の中間値の左半分を表す。

【００５６】

こうして得られた中間値を用いて、ラウンド鍵：$K1_1$，$K1_2$，$K1_3$，$K1_4$，$K2_1$，．．．，$K7_1$，$K7_2$は、以下のように表せる。

【００５７】

【数１３】

$$K1_1=Z0_1+V1$$
$$K1_2=Z1_3+V1$$
$$K1_3=Z1_4+V1$$
$$K1_4=Z0_2+Z1_4$$
$$K2_1=Z1_1+V2$$
$$K2_2=Z2_3+V2$$
$$K2_3=Z2_4+V2$$
$$K2_4=Z1_2+Z2_4$$
$$K3_1=Z2_1+V3$$
$$K3_2=Z3_3+V3$$
$$K3_3=Z3_4+V3$$
$$K3_4=Z2_2+Z3_4$$
$$K4_1=Z3_1+V4$$
$$K4_2=Z4_3+V4$$
$$K4_3=Z4_4+V4$$
$$K4_4=Z3_2+Z4_4$$
$$K5_1=Z5_1+Z4_3$$
$$K5_2=W5_1+V5$$
$$K5_3=W5_2+V5$$
$$K5_4=Z4_1+W5_2$$
$$K6_1=Z6_1+Z5_3$$
$$K6_2=W6_1+V6$$
$$K6_3=W6_2+V6$$
$$K6_4=Z5_1+W6_2$$

$K7_1 = Z7_1 + Z6_3$

$K7_2 = W7_1 + V7$

$K7_3 = W7_2 + V7$

$K7_4 = Z6_1 + W7_2$

【００５８】

なお、$K1_1$，$K1_2$，$K1_3$，$K1_4$，$K2_1$，．．．，$K7_1$，$K7_2$は、４つの要素から成るベクトルである。

【００５９】

次に、図１に示すステップＳ１０２の中間変数消去処理ステップについて説明する。上述の４つの要素から成るベクトル$K1_1$，$K1_2$，$K1_3$，$K1_4$，$K2_1$，．．．，$K7_1$，$K7_2$について、実際に各値を代入して計算すると、以下のような式が得られる。

【００６０】

【数１４】

$$K1_1 = \begin{pmatrix} v11 + z21 \\ v12 + z22 \\ v13 + z23 \\ v14 + z24 \end{pmatrix}$$

$$K1_2 = \begin{pmatrix} h01 + h11 + h03 + v11 + z32 + z41 \\ h01 + h02 + h12 + h04 + v12 + z33 + z42 \\ h01 + h02 + h03 + h13 + v13 + z31 + z34 + z43 \\ h02 + h04 + h14 + v14 + z31 + z44 \end{pmatrix}$$

$$K1_3 = \begin{pmatrix} h02 + h04 + v11 + z31 \\ h01 + h03 + v12 + z32 \\ h02 + h03 + h04 + v13 + z32 + z41 + z33 \\ h01 + h02 + h03 + v14 + z31 + z34 + z44 \end{pmatrix}$$

$$K1_4 = \begin{pmatrix} h02 + h04 + v01 + z11 + z31 \\ h01 + h03 + v02 + z12 + z32 \\ h02 + h03 + h04 + v03 + z13 + z32 + z41 + z33 \\ h01 + h02 + h03 + v04 + z31 + z14 + z34 + z44 \end{pmatrix}$$

$$K2_1 = \begin{pmatrix} v01 + v21 + z11 \\ v02 + v22 + z12 \\ v03 + v23 + z13 \\ v04 + v24 + z14 \end{pmatrix}$$

$$K2_2 = \begin{pmatrix} h02 + h11 + h03 + h21 + h13 + v21 + z33 + z34 + z43 \\ h11 + h03 + h12 + h04 + h22 + h14 + v22 + z31 + z41 + z33 + z42 + z34 \\ h11 + h12 + h04 + h13 + h23 + v23 + z32 + z42 + z34 + z43 \\ h01 + h02 + h12 + h14 + h24 + v24 + z32 + z33 + z42 + z34 \end{pmatrix}$$

$$K2_3 = \begin{pmatrix} h01 + h12 + h14 + v21 + z31 + z33 + z42 + z44 \\ h02 + h11 + h13 + v22 + z31 + z32 + z41 + z34 + z43 \\ h02 + h12 + h13 + h14 + v23 + z31 + z32 + z41 + z42 + z34 + z43 + z44 \\ h01 + h02 + h11 + h12 + h04 + h13 + v24 + z41 + z33 + z42 + z43 + z44 \end{pmatrix}$$

$$K2_4 = \begin{pmatrix} h01 + h12 + h14 + v11 + z21 + z31 + z33 + z42 + z44 \\ h02 + h11 + h13 + v12 + z22 + z31 + z32 + z41 + z34 + z43 \\ h02 + h12 + h13 + h14 + v13 + z31 + z23 + z32 + z41 + z42 + z34 + z43 + z44 \\ h01 + h02 + h11 + h12 + h04 + h13 + v14 + z41 + z24 + z33 + z42 + z43 + z44 \end{pmatrix}$$

$$K3_1 = \begin{pmatrix} v11+v31+z21 \\ v12+v32+z22 \\ v13+v33+z23 \\ v14+v34+z24 \end{pmatrix}$$

$$K3_2 = \begin{pmatrix} h01+h03+h12+h21+h04+h13+h31+h23+v31+z41+z42+z34+z43 \\ h01+h21+h13+h22+h14+h32+h24+v32+z31+z41+z33+z43 \\ h01+h02+h21+h22+h14+h23+h33+v33+z32+z41+z33+z34 \\ h02+h11+h03+h12+h22+h24+h34+v34+z41+z33+z42+z34+z44 \end{pmatrix}$$

$$K3_3 = \begin{pmatrix} h01+h02+h11+h03+h04+h22+h24+v31+z31+z32+z41 \\ h02+h03+h12+h21+h04+h23+v32+z32+z33+z42 \\ h03+h12+h22+h23+h24+v33+z31+z32+z33+z42 \\ h01+h02+h11+h12+h21+h04+h22+h14+h23+v34+z41+z33+z42+z44 \end{pmatrix}$$

$$K3_4 = \begin{pmatrix} h01+h02+h11+h03+h04+h22+h24+v01+v21+z11+z31+z32+z41 \\ h02+h03+h12+h21+h04+h23+v02+v22+z12+z32+z33+z42 \\ h03+h12+h22+h23+h24+v03+v23+z13+z31+z32+z33+z42 \\ h01+h02+h11+h12+h21+h04+h22+h14+h23+v04+v24+z14+z41+z33 \\ +z42+z44 \end{pmatrix}$$

$$k4_1 = \begin{pmatrix} v01+v21+v41+z11 \\ v02+v22+v42+z12 \\ v03+v23+v43+z13 \\ v04+v24+v44+z14 \end{pmatrix}$$

$$k4_2 = \begin{pmatrix} h01+h11+h03+h13+h22+h31+h14+h23+h41+h33+v41+z32+z41+z43 \\ h11+h31+h23+h32+h24+h42+h34+v42+z41 \\ h02+h11+h12+h04+h31+h32+h24+h33+h43+v43+z31+z42 \\ h02+h12+h21+h13+h22+h32+h34+h44+v44+z31+z32+z41+z42+z34 \\ +z43 \end{pmatrix}$$

$$k4_3 = \begin{pmatrix} h01+h02+h11+h03+h12+h21+h13+h14+h32+h34+v41+z31+z42+z34 \\ +z43+z44 \\ h02+h03+h12+h04+h13+h22+h31+h14+h33+v42+z32+z33+z42+z43 \\ h01+h02+h03+h04+h13+h22+h32+h33+h34+v43+z31+z32+z43+z44 \\ h02+h11+h12+h21+h04+h22+h31+h14+h32+h24+h33+v44+z31+z42 \\ +z44 \end{pmatrix}$$

$$k4_4 = \begin{pmatrix} h01+h02+h11+h03+h12+h21+h13+h14+h32+h34+v11+v31+z21+z31 \\ +z42+z34+z43+z44 \\ h02+h03+h12+h04+h13+h22+h31+h14+h33+v12+v32+z22+z32+z33 \\ +z42+z43 \\ h01+h02+h03+h04+h13+h22+h32+h33+h34+v13+v33+z31+z23+z32 \\ +z43+z44 \\ h02+h11+h12+h21+h04+h22+h31+h14+h32+h24+h33+v14+v34+z31 \\ +z24+z42+z44 \end{pmatrix}$$

$$K5_1 = \begin{pmatrix} h01+h11+h03+h13+h22+h31+h14+h23+h41+h33+v01+v21+v41+v51 \\ +z11+z32+z41+z43 \\ h11+h31+h23+h32+h24+h42+h34+v02+v22+v42+v52+z12+z41 \\ h02+h11+h12+h04+h31+h32+h24+h33+h43+v03+v23+v43+v53+z13 \\ +z31+z42 \\ h02+h12+h21+h13+h22+h32+h34+h44+v04+v24+v44+z31+v54+z14 \\ +z32+z41+z42+z34+z43 \end{pmatrix}$$

$$K5_2 = \begin{pmatrix} h02+h11+h12+h21+h13+h22+h31+h23+h24+v51+z31+z32+z42+z34 \\ +z43 \\ h01+h02+h03+h12+h04+h13+h22+h14+h23+h32+h24+v52+z31+z32 \\ +z41+z42+z43 \\ h01+h02+h03+h12+h21+h14+h24+h33+v53+z31+z41+z42+z34 \\ h01+h03+h21+h04+h14+h23+h24+h34+v54+z34 \end{pmatrix}$$

$$K5_3 = \begin{pmatrix} h11+h12+h21+h04+h22+h14+h33+v51+z32+z42+z34 \\ h01+h02+h12+h14+h24+h34+v52+z32+z33+z42+z34 \\ h02+h11+h03+h21+h13+h31+v53+z33+z34+z43 \\ h11+h03+h21+h13+h32+h24+z31+v54+z32+z33+z43+z44 \end{pmatrix}$$

$$K5_4 = \begin{pmatrix} h11+h12+h21+h04+h22+h14+h33+v11+v31+z21+z32+z42+z34 \\ h01+h02+h12+h14+h24+h34+v12+v32+z22+z32+z33+z42+z34 \\ h02+h11+h03+h21+h13+h31+v13+v33+z23+z33+z34+z43 \\ h11+h03+h21+h13+h32+h24+v14+v34+z31+z32+z24+z33+z43+z44 \end{pmatrix}$$

$$K6_1 = \begin{pmatrix} h01+h03+h12+h21+h04+h13+h31+h23+v11+v31+v61+z21+z41+z42 \\ +z34+z43 \\ h01+h21+h13+h22+h14+h32+h24+v12+v32+v62+z22+z31+z41+z33 \\ +z43 \\ h01+h02+h21+h22+h14+h23+h33+v13+v33+v63+z23+z32+z41+z33 \\ +z34 \\ h02+h11+h03+h12+h22+h24+h34+v14+v34+z41+v64+z24+z33+z42 \\ +z34+z44 \end{pmatrix}$$

$$K6_2 = \begin{pmatrix} h01+h02+h11+h03+h12+h21+h13+h14+v61+z31+z42+z34+z43+z44 \\ h02+h03+h12+h04+h13+h22+h14+v62+z32+z33+z42+z43 \\ h02+h11+h04+h14+h23+z31+v63+z41+z44 \\ h11+h04+h13+h14+h24+z32+z41+v64+z34+z43+z44 \end{pmatrix}$$

$$K6_3 = \begin{pmatrix} h01+h02+h11+h12+h04+h23+v61+z41+z33+z42 \\ h02+h04+h14+h24+v62+z31+z44 \\ h01+h11+h03+h21+v63+z32+z41 \\ h01+h11+h03+h22+h14+z32+z41+v64+z44 \end{pmatrix}$$

$$K6_4 = \begin{pmatrix} h01+h02+h11+h12+h04+h23+v01+v21+v41+v51+z11+z41+z33+z42 \\ h02+h04+h14+h24+v02+v22+v42+v52+z12+z31+z44 \\ h01+h11+h03+h21+v03+v23+v43+v53+z13+z32+z41 \\ h01+h11+h03+h22+h14+v04+v24+v44+v54+z14+z32+z41+z44 \end{pmatrix}$$

$$K7_1 = \begin{pmatrix} h02+h11+h03+h21+h13+v01+v21+v41+v51+z11+v71+z33+z34+z43 \\ h11+h03+h12+h04+h22+h14+v02+v22+v42+v52+z12+z31+v72+z41 \\ +z33+z42+z34 \\ h11+h12+h04+h13+h23+v03+v23+v43+v53+z13+z32+v73+z42+z34 \\ +z43 \\ h01+h02+h12+h14+h24+v04+v24+v44+v54+z14+z32+z33+z42+v74 \\ +z34 \end{pmatrix}$$

$$K7_2 = \begin{pmatrix} h01+h02+h11+h03+h04+v71+z31+z32+z41 \\ h02+h03+h12+h04+v72+z32+z33+z42 \\ h01+h04+h13+z31+z32+z41+v73+z33+z34+z43 \\ h01+h03+h04+h14+v74+z34 \end{pmatrix}$$

【００６１】

次に、ステップＳ１０３の変数移項処理を実行する。上記Ｋ１$_1$，Ｋ１$_2$，Ｋ１$_3$，Ｋ１$_4$，Ｋ２$_1$，．．．，Ｋ７$_1$，Ｋ７$_2$の結果に基づいて、上記の連立線形方程式を変形し、右辺がｚｘｘ，ｖｘｘの項のみを含むように変形すると、以下のように表すことができる。

【００６２】

【数１５】

$$
\begin{aligned}
&k1_{11} = v11 + z21\\
&k1_{12} = v12 + z22\\
&k1_{13} = v13 + z23\\
&k1_{14} = v14 + z24\\
&h01 + h11 + h03 + k1_{21} = v11 + z32 + z41\\
&h01 + h02 + h12 + h04 + k1_{22} = v12 + z33 + z42\\
&h01 + h02 + h03 + h13 + k1_{23} = v13 + z31 + z34 + z43\\
&h02 + h04 + h14 + k1_{24} = v14 + z31 + z44\\
&h02 + h04 + k1_{31} = v11 + z31\\
&h01 + h03 + k1_{32} = v12 + z32\\
&h02 + h03 + h04 + k1_{33} = v13 + z32 + z41 + z33\\
&h01 + h02 + h03 + k1_{34} = v14 + z31 + z34 + z44\\
&h02 + h04 + k1_{41} = v01 + z11 + z31
\end{aligned}
$$

$$h01+h03+k1_{42}=v02+z12+z32$$
$$h02+h03+h04+k1_{43}=v03+z13+z32+z41+z33$$
$$h01+h02+h03+k1_{44}=v04+z31+z14+z34+z44$$
$$k2_{11}=v01+v21+z11$$
$$k2_{12}=v02+v22+z12$$
$$k2_{13}=v03+v23+z13$$
$$k2_{14}=v04+v24+z14$$
$$h02+h11+h03+h21+h13+k2_{21}=v21+z33+z34+z43$$
$$h11+h03+h12+h04+h22+h14+k2_{22}=v22+z31+z41+z33+z42+z34$$
$$h11+h12+h04+h13+h23+k2_{23}=v23+z32+z42+z34+z43$$
$$h01+h02+h12+h14+h24+k2_{24}=v24+z32+z33+z42+z34$$
$$h01+h12+h14+k2_{31}=v21+z31+z33+z42+z44$$
$$h02+h11+h13+k2_{32}=v22+z31+z32+z41+z34+z43$$
$$h02+h12+h13+h14+k2_{33}=v23+z31+z32+z41+z42+z34+z43+z44$$
$$h01+h02+h11+h12+h04+h13+k2_{34}=v24+z41+z33+z42+z43+z44$$
$$h01+h12+h14+k2_{41}=v11+z21+z31+z33+z42+z44$$
$$h02+h11+h13+k2_{42}=v12+z22+z31+z32+z41+z34+z43$$
$$h02+h12+h13+h14+k2_{43}=v13+z31+z23+z32+z41+z42+z34+z43+z44$$
$$h01+h02+h11+h12+h04+h13+k2_{44}=v14+z41+z24+z33+z42+z43+z44$$
$$k3_{11}=v11+v31+z21$$
$$k3_{12}=v12+v32+z22$$
$$k3_{13}=v13+v33+z23$$
$$k3_{14}=v14+v34+z24$$
$$h01+h03+h12+h21+h04+h13+h31+h23+k3_{21}=v31+z41+z42+z34+z43$$
$$h01+h21+h13+h22+h14+h32+h24+k3_{22}=v32+z31+z41+z33+z43$$
$$h01+h02+h21+h22+h14+h23+h33+k3_{23}=v33+z32+z41+z33+z34$$
$$h02+h11+h03+h12+h22+h24+h34+k3_{24}=v34+z41+z33+z42+z34+z44$$
$$h01+h02+h11+h03+h04+h22+h24+k3_{31}=v31+z31+z32+z41$$
$$h02+h03+h12+h21+h04+h23+k3_{32}=v32+z32+z33+z42$$
$$h03+h12+h22+h23+h24+k3_{33}=v33+z31+z32+z33+z42$$
$$h01+h02+h11+h12+h21+h04+h22+h14+h23+k3_{34}=v34+z41+z33+z42+z44$$
$$h01+h02+h11+h03+h04+h22+h24+k3_{41}=v01+v21+z11+z31+z32+z41$$
$$h02+h03+h12+h21+h04+h23+k3_{42}=v02+v22+z12+z32+z33+z42$$

$h03+h12+h22+h23+h24+k3_{43} = v03+v23+z13+z31+z32+z33+z42$

$h01 + h02 + h11 + h12 + h21 + h04 + h22 + h14 + h23 + k3_{44} = v04 + v24 + z14 + z41 + z33 + z42 + z44$

$k4_{11} = v01 + v21 + v41 + z11$

$k4_{12} = v02 + v22 + v42 + z12$

$k4_{13} = v03 + v23 + v43 + z13$

$k4_{14} = v04 + v24 + v44 + z14$

$h01 + h11 + h03 + h13 + h22 + h31 + h14 + h23 + h41 + h33 + k4_{21} = v41 + z32 + z41 + z43$

$h11 + h31 + h23 + h32 + h24 + h42 + h34 + k4_{22} = v42 + z41$

$h02+h11+h12+h04+h31+h32+h24+h33+h43+k4_{23} = v43+z31+z42$

$h02 + h12 + h21 + h13 + h22 + h32 + h34 + h44 + k4_{24} = v44 + z31 + z32 + z41 + z42 + z34 + z43$

$h01 + h02 + h11 + h03 + h12 + h21 + h13 + h14 + h32 + h34 + k4_{31} = v41 + z31 + z42 + z34 + z43 + z44$

$h02 + h03 + h12 + h04 + h13 + h22 + h31 + h14 + h33 + k4_{32} = v42 + z32 + z33 + z42 + z43$

$h01 + h02 + h03 + h04 + h13 + h22 + h32 + h33 + h34 + k4_{33} = v43 + z31 + z32 + z43 + z44$

$h02+h11+h12+h21+h04+h22+h31+h14+h32+h24+h33+k4_{34} = v44 + z31 + z42 + z44$

$h01 + h02 + h11 + h03 + h12 + h21 + h13 + h14 + h32 + h34 + k4_{41} = v11 + v31 + z21 + z31 + z42 + z34 + z43 + z44$

$h02 + h03 + h12 + h04 + h13 + h22 + h31 + h14 + h33 + k4_{42} = v12 + v32 + z22 + z32 + z33 + z42 + z43$

$h01 + h02 + h03 + h04 + h13 + h22 + h32 + h33 + h34 + k4_{43} = v13 + v33 + z31 + z23 + z32 + z43 + z44$

$h02+h11+h12+h21+h04+h22+h31+h14+h32+h24+h33+k4_{44} = v14 + v34 + z31 + z24 + z42 + z44$

$h01 + h11 + h03 + h13 + h22 + h31 + h14 + h23 + h41 + h33 + k5_{11} = v01 + v21 + v41 + v51 + z11 + z32 + z41 + z43$

$h11 + h31 + h23 + h32 + h24 + h42 + h34 + k5_{12} = v02 + v22 + v42 + v52 + z12 + z41$

$h02 + h11 + h12 + h04 + h31 + h32 + h24 + h33 + h43 + k5_{13} = v03 + v23 + v43 + v53 + z13 + z31 + z42$

$h02 + h12 + h21 + h13 + h22 + h32 + h34 + h44 + k5_{14} = v04 + v24 + v44 + z31 + v54 + z14 + z32 + z41 + z42 + z34 + z43$

$h02 + h11 + h12 + h21 + h13 + h22 + h31 + h23 + h24 + k5_{21} = v51 + z31 + z32 + z42 + z34 + z43$

$h01+h02+h03+h12+h04+h13+h22+h14+h23+h32+h24+k5_{22}=v52+z31+z32+z41+z42+z43$

$h01+h02+h03+h12+h21+h14+h24+h33+k5_{23}=v53+z31+z41+z42+z34$

$h01+h03+h21+h04+h14+h23+h24+h34+k5_{24}=v54+z34$

$h11+h12+h21+h04+h22+h14+h33+k5_{31}=v51+z32+z42+z34$

$h01+h02+h12+h14+h24+h34+k5_{32}=v52+z32+z33+z42+z34$

$h02+h11+h03+h21+h13+h31+k5_{33}=v53+z33+z34+z43$

$h11+h03+h21+h13+h32+h24+z31+k5_{34}=v54+z32+z33+z43+z44$

$h11+h12+h21+h04+h22+h14+h33+k5_{41}=v11+v31+z21+z32+z42+z34$

$h01+h02+h12+h14+h24+h34+k5_{42}=v12+v32+z22+z32+z33+z42+z34$

$h02+h11+h03+h21+h13+h31+k5_{43}=v13+v33+z23+z33+z34+z43$

$h11+h03+h21+h13+h32+h24+k5_{44}=v14+v34+z31+z32+z24+z33+z43+z44$

$h01+h03+h12+h21+h04+h13+h31+h23+k6_{11}=v11+v31+v61+z21+z41+z42+z34+z43$

$h01+h21+h13+h22+h14+h32+h24+k6_{12}=v12+v32+v62+z22+z31+z41+z33+z43$

$h01+h02+h21+h22+h14+h23+h33+k6_{13}=v13+v33+v63+z23+z32+z41+z33+z34$

$h02+h11+h03+h12+h22+h24+h34+k6_{14}=v14+v34+z41+v64+z24+z33+z42+z34+z44$

$h01+h02+h11+h03+h12+h21+h13+h14+k6_{21}=v61+z31+z42+z34+z43+z44$

$h02+h03+h12+h04+h13+h22+h14+k6_{22}=v62+z32+z33+z42+z43$

$h02+h11+h04+h14+h23+z31+k6_{23}=v63+z41+z44$

$h11+h04+h13+h14+h24+z32+z41+k6_{24}=v64+z34+z43+z44$

$h01+h02+h11+h12+h04+h23+k6_{31}=v61+z41+z33+z42$

$h02+h04+h14+h24+k6_{32}=v62+z31+z44$

$h01+h11+h03+h21+k6_{33}=v63+z32+z41$

$h01+h11+h03+h22+h14+z32+z41+k6_{34}=v64+z44$

$h01+h02+h11+h12+h04+h23+k6_{41}=v01+v21+v41+v51+z11+z41+z33+z42$

$h02+h04+h14+h24+k6_{42}=v02+v22+v42+v52+z12+z31+z44$

$h01+h11+h03+h21+k6_{43}=v03+v23+v43+v53+z13+z32+z41$

$h01+h11+h03+h22+h14+k6_{44}=v04+v24+v44+v54+z14+z32+z41+z44$

$$h02+h11+h03+h21+h13+k7_{11}=v01+v21+v41+v51+z11+v71+z33+z34+z43$$

$$h11+h03+h12+h04+h22+h14+k7_{12}=v02+v22+v42+v52+z12+z31+v72+z41+z33+z42+z34$$

$$h11+h12+h04+h13+h23+k7_{13}=v03+v23+v43+v53+z13+z32+v73+z42+z34+z43$$

$$h01+h02+h12+h14+h24+k7_{14}=v04+v24+v44+v54+z14+z32+z33+z42+v74+z34$$

$$h01+h02+h11+h03+h04+k7_{21}=v71+z31+z32+z41$$

$$h02+h03+h12+h04+k7_{22}=v72+z32+z33+z42$$

$$h01+h04+h13+z31+z32+z41+k7_{23}=v73+z33+z34+z43$$

$$h01+h03+h04+h14+k7_{24}=v74+z34$$

【００６３】

次に、ステップＳ１０４の行列方程式変換処理を実行する。ここで、ベクトルＫ，Ｈ，Ｕ，Ｖを下記のように設定する。

【００６４】

【数１６】

Ｋ＝（ｋ１$_{11}$，Ｋ１$_{12}$，．．．，ｋ７$_{24}$）

Ｈ＝（ｈ０１，ｈ０２，．．．，ｈ４４）

Ｕ＝（ｚ１１，ｚ１２，．．．，ｚ４４）

Ｖ＝（ｖ０１，ｖ０２，．．．ｖ７４）

【００６５】

上記式のように、ベクトルＫ，Ｈ，Ｕ，Ｖを設定すると、上記連立線形方程式は以下のように行列方程式に変換できる。

【００６６】

【数１７】

$$M_{KH}\begin{pmatrix}{}^tK\\{}^tH\end{pmatrix}=M_{UV}\begin{pmatrix}{}^tU\\{}^tV\end{pmatrix}$$

【００６７】

なお、上記式において、M_{KH}，M_{UV}は、上記連立線形方程式の係数から成るＧＦ（２）上の行列である。

【００６８】

次に、ステップＳ１０５のユニタリ変換処理を実行する。

【００６９】

【数１８】

$$rank(M_{UV}) = N_r$$

【００７０】

とする。また、行列M_{UV}の行数をN_mとする。上記行列方程式の両辺に左から行変形ユニタリー行列Ｑを乗ずることによって、行列M_{UV}を階段行列に変形することができる。このとき、QM_{UV}のうち、下$N_m - N_r$行から成る小行列は零行列になる。

【００７１】

次に、ステップＳ１０６の小行列選択処理を実行する。QM_{KH}の下$N_m - N_r$行の小行列をM^*_{KH}とおくと、M^*_{KH}はゼロ行列（Ｏ）であり、下記式によって示される。

【００７２】

【数１９】

$$M^*_{KH} = O$$

【００７３】

次にステップＳ１０７の線形関係式生成処理を実行する。この行列方程式を行毎の線形関係式に変換し、h01,h02,．．．,h44の具体的値を代入すると、以下のような関係式が得られる。

【００７４】

【数２０】

$$0xc7 = k1_{11} + k1_{21} + k1_{22} + k1_{24} + k1_{31} + k1_{32} + k1_{34} + k1_{42} + k1_{44} + k2_{12} + k2_{14} + k2_{22} + k2_{24} + k2_{41}$$

$$0x33 = k1_{12} + k1_{21} + k1_{22} + k1_{23} + k1_{31} + k1_{32} + k1_{33} + k1_{41} + k1_{43} + k2_{11} + k2_{13} + k2_{21} + k2_{23} + k2_{42}$$

$$0x48 = k1_{13} + k1_{22} + k1_{24} + k1_{32} + k1_{34} + k1_{41} + k1_{42} + k1_{44} + k2_{11} + k2_{12} + k2_{14} + k2_{21} + k2_{22} + k2_{24} + k2_{43}$$

$$0xef = k1_{14} + k1_{21} + k1_{22} + k1_{23} + k1_{24} + k1_{31} + k1_{32} + k1_{33} + k1_{34} + k1_{41} + k1_{43} + k1_{44} + k2_{11} + k2_{13} + k2_{14} + k2_{21} + k2_{23} + k2_{24} + k2_{44}$$

$$0xc7 = k1_{21} + k1_{31} + k2_{11} + k3_{41}$$

$$0x33 = k1_{22} + k1_{32} + k2_{12} + k3_{42}$$

$$0x00 = k1_{23} + k1_{33} + k1_{41} + k2_{12} + k2_{13} + k2_{21} + k3_{41} + k3_{42} + k3_{43}$$

$$0xd4 = k1_{24} + k1_{34} + k1_{43} + k2_{11} + k2_{12} + k2_{13} + k2_{23} + k3_{42} + k4_{11} + k4_{21}$$

$$0xc7 = k1_{41} + k1_{42} + k2_{21} + k2_{22} + k3_{42} + k3_{43} + k4_{11} + k4_{13} + k4_{21} + k4_{23}$$

$$0x74 = k1_{42} + k1_{43} + k2_{11} + k2_{12} + k2_{22} + k2_{23} + k3_{42} + k3_{43} + k4_{11} + k4_{12} + k4_{21} + k4_{22}$$

$$0x65 = k1_{43} + k2_{12} + k2_{14} + k2_{23} + k3_{42} + k4_{13} + k4_{14} + k4_{23} + k4_{24}$$

$$0x33 = k1_{44} + k2_{11} + k2_{24} + k3_{41} + k3_{44}$$

$$0x8a = k2_{11} + k2_{12} + k3_{42} + k3_{44} + k4_{11} + k4_{14} + k4_{24} + k4_{31}$$

$$0xf7 = k2_{12} + k2_{13} + k3_{41} + k3_{43} + k4_{11} + k4_{12} + k4_{21} + k4_{32}$$

$$0x29 = k2_{13} + k2_{14} + k3_{41} + k3_{42} + k3_{44} + k4_{11} + k4_{12} + k4_{13} + k4_{21} + k4_{22} + k4_{33}$$

$$0xa1 = k2_{14} + k3_{41} + k3_{44} + k4_{11} + k4_{22} + k4_{23} + k4_{24} + k4_{31} + k4_{32} + k4_{33} + k4_{34}$$

$$0x41 = k2_{21} + k2_{31} + k3_{41} + k3_{43} + k3_{44} + k4_{11} + k4_{13} + k4_{14} + k4_{23} + k4_{31} + k4_{34}$$

$$0x74 = k2_{22} + k2_{32} + k3_{41} + k3_{42} + k3_{43} + k4_{11} + k4_{12} + k4_{13} + k4_{23} + k4_{24} + k4_{31} + k4_{32} + k4_{34}$$

$$0xf4 = k2_{23} + k2_{33} + k3_{41} + k3_{42} + k3_{43} + k3_{44} + k4_{11} + k4_{12} + k4_{13} + k4_{14} + k4_{24} + k4_{31} + k4_{32} + k4_{33}$$

$$0x57 = k2_{24} + k2_{34} + k4_{24} + k4_{34}$$

$$0xf6 = k2_{41} + k3_{11} + k3_{21} + k3_{41} + k3_{42} + k3_{43} + k4_{11} + k4_{12} + k4_{13} + k4_{21} + k4_{23} + k4_{24} + k4_{32} + k4_{34}$$

$$0x7c = k2_{42} + k3_{12} + k3_{22} + k3_{42} + k4_{12} + k4_{22} + k4_{23} + k4_{24} + k4_{33} + k4_{34}$$

$$0x43 = k2_{43} + k3_{13} + k3_{23} + k3_{41} + k3_{42} + k3_{43} + k4_{11} + k4_{12} + k4_{13} + k4_{21} + k4_{32} + k4_{33}$$

$$0x5f = k2_{44} + k3_{14} + k3_{24} + k3_{43} + k4_{13} + k4_{22} + k4_{24} + k4_{32} + k4_{33} + k4_{34}$$

$$0x7d = k3_{11} + k3_{41} + k3_{42} + k3_{43} + k3_{44} + k4_{11} + k4_{12} + k4_{13} + k4_{14} + k4_{21} + k4_{24} + k4_{32} + k4_{33} + k5_{41}$$

$$0x2b = k3_{12} + k3_{41} + k3_{42} + k4_{11} + k4_{12} + k4_{22} + k4_{23} + k4_{31} + k4_{33} + k5_{42}$$

$$0x02 = k3_{13} + k3_{44} + k4_{14} + k4_{21} + k4_{23} + k4_{31} + k4_{33} + k4_{34} + k5_{43}$$

$$0xdc = k3_{14} + k3_{42} + k3_{43} + k3_{44} + k4_{12} + k4_{13} + k4_{14} + k4_{22} + k4_{33} + k4_{34} + k5_{44}$$

$$0x8a = k3_{21} + k3_{31} + k3_{42} + k3_{43} + k3_{44} + k4_{12} + k4_{13} + k4_{14} + k4_{24} + k4_{32} + k4_{33}$$

$$0x7f = k3_{22} + k3_{32} + k3_{41} + k3_{42} + k3_{43} + k3_{44} + k4_{11} + k4_{12} + k4_{13} + k4_{14} + k4_{23} + k4_{24} + k4_{31} + k4_{32}$$

$$0x88 = k3_{23} + k3_{33} + k3_{41} + k3_{42} + k4_{11} + k4_{12} + k4_{21} + k4_{23} + k4_{24} + k4_{32} + k4_{33} + k4_{34}$$

$$0x54 = k3_{24} + k3_{34} + k3_{42} + k3_{43} + k4_{12} + k4_{13} + k4_{22} + k4_{24} + k4_{33} + k4_{34}$$

$$0x7f = k3_{41} + k3_{42} + k4_{12} + k4_{21} + k4_{23} + k4_{24} + k4_{32} + k4_{33} + k4_{34} + k5_{11} + k5_{21}$$

$$0x7f = k3_{42} + k4_{11} + k4_{12} + k4_{13} + k4_{21} + k4_{24} + k4_{31} + k4_{32} + k4_{34} + k5_{11} + k5_{13} + k5_{21} + k5_{23}$$

$$0x8a = k3_{43} + k3_{44} + k4_{11} + k4_{13} + k4_{21} + k4_{31} + k4_{33} + k4_{34} + k5_{11} + k5_{14} + k5_{21} + k5_{24}$$

$$0x00 = k3_{44} + k4_{12} + k4_{14} + k4_{22} + k4_{32} + k4_{34} + k5_{12} + k5_{22}$$

$$0xf7 = k4_{11} + k4_{13} + k4_{23} + k4_{33} + k4_{41} + k5_{11} + k5_{13} + k5_{21} + k5_{23} + k5_{41}$$

$$0x29 = k4_{12} + k4_{13} + k4_{14} + k4_{21} + k4_{23} + k4_{24} + k4_{31} + k4_{33} + k4_{34} + k4_{41} + k4_{42} + k5_{12} + k5_{13} + k5_{14} + k5_{22} + k5_{23} + k5_{24} + k5_{41} + k5_{42}$$

$$0x2b = k4_{13} + k4_{14} + k4_{22} + k4_{24} + k4_{32} + k4_{34} + k4_{42} + k4_{43} + k5_{13} + k5_{14} + k5_{23} + k5_{24} + k5_{42} + k5_{43}$$

$$0x88 = k4_{14} + k4_{21} + k4_{23} + k4_{31} + k4_{33} + k4_{41} + k4_{43} + k4_{44} + k5_{14} + k5_{24} + k5_{41} + k5_{43} + k5_{44}$$

$$0x43 = k4_{21} + k4_{31} + k5_{41} + k6_{11} + k6_{21}$$

$$0xc0 = k4_{22} + k4_{24} + k4_{32} + k4_{34} + k4_{41} + k4_{42} + k4_{44} + k5_{44} + k6_{11} + k6_{12} + k6_{21} + k6_{32}$$

$$0xcb = k4_{23} + k4_{24} + k4_{33} + k4_{34} + k4_{41} + k5_{43} + k6_{11} + k6_{13} + k6_{21} + k6_{33}$$

$$0x81 = k4_{24} + k4_{34} + k4_{42} + k4_{43} + k5_{43} + k6_{12} + k6_{22}$$

$$0x7e = k4_{41} + k5_{41} + k5_{43} + k6_{13} + k6_{23}$$

$$0xdd = k4_{42} + k4_{43} + k4_{44} + k5_{42} + k5_{43} + k6_{14} + k6_{24}$$

$$0x00 = k4_{43} + k4_{44} + k5_{43} + k6_{14} + k6_{34}$$

$$0x00 = k4_{44} + k5_{41} + k5_{44} + k6_{11} + k6_{31}$$

$$0xf7 = k5_{11} + k5_{41} + k6_{11} + k6_{31} + k6_{41}$$

$$0x14 = k5_{12} + k5_{41} + k5_{43} + k5_{44} + k6_{11} + k6_{13} + k6_{14} + k6_{21} + k6_{23} + k6_{34} + k6_{42}$$

$$0x23 = k5_{13} + k5_{41} + k5_{42} + k6_{11} + k6_{12} + k6_{22} + k6_{24} + k6_{31} + k6_{34} + k6_{43}$$

$$0x8a = k5_{14} + k5_{44} + k6_{14} + k6_{34} + k6_{44}$$

$$0xb4 = k5_{21} + k5_{31} + k5_{41} + k5_{42} + k6_{11} + k6_{12} + k6_{21} + k6_{32}$$

$$0x0b = k5_{22} + k5_{32} + k5_{42} + k5_{43} + k6_{12} + k6_{13} + k6_{22} + k6_{33}$$

$$0x00 = k5_{23} + k5_{33} + k5_{41} + k5_{42} + k5_{44} + k6_{11} + k6_{12} + k6_{14} + k6_{31} + k6_{32} + k6_{34}$$

$$0x00 = k5_{24} + k5_{34} + k5_{41} + k5_{43} + k5_{44} + k6_{11} + k6_{13} + k6_{14} + k6_{31} + k6_{33} + k6_{34}$$

$$0xc7 = k5_{41} + k5_{42} + k5_{43} + k5_{44} + k6_{11} + k6_{12} + k6_{13} + k6_{14} + k6_{21} + k6_{23} + k6_{32} + k6_{34} + k6_{41} + k7_{11} + k7_{21}$$

$$0xfc = k5_{42} + k6_{12} + k6_{21} + k6_{31} + k6_{32} + k6_{43} + k7_{13} + k7_{23}$$

$$0x18 = k5_{43} + k5_{44} + k6_{13} + k6_{14} + k6_{21} + k6_{22} + k6_{31} + k6_{32} + k6_{33} + k6_{34} + k6_{43} + k6_{44} + k7_{13} + k7_{14} + k7_{23} + k7_{24}$$

$$0xf4 = k6_{21} + k6_{22} + k6_{23} + k6_{24} + k6_{31} + k6_{32} + k6_{33} + k6_{34} + k6_{41} + k6_{42} + k7_{11} + k7_{12} + k7_{21} + k7_{22}$$

【００７５】

ここで、下記式が成立する。

【００７６】

【数２１】

$$rank\ (M^*_{KH}) = N_m - N_r$$

【００７７】

従って、上記６０個の線形関係式は、互いに独立な線形関係式である。従って、これら６０個のＧＦ（２）上の任意を線形結合して得られる$2^{60}-1$個の線形関係式が成り立つことがわかる。この線形関係式が多ければ、暗号の設計者の意図しない新たな攻撃を招く恐れがあるので、上述した方法によって得られた線形関係式の総数を、暗号強度評価の一つの指標として用いることができる。

【００７８】

［暗号強度指標算出処理具体例２］

次に、本発明に係る暗号強度指標算出処理の第２の具体例として、東芝から提案されたブロック暗号「Hierocrypt-３」に対して本発明に係る暗号強度評価方法を適用した処理例の詳細について説明する。Hierocrypt-３は、AES互換の暗号であり、ブロック長は128bit、鍵長は、128,192,256 の何れかである。以下に説明する処理例は、鍵長が 256 bitである場合についての処理例である。

【００７９】

まず、図１に示すステップＳ１０１の暗号処理アルゴリズムの設定ステップについて説明する。ここでは、東芝から提案されたブロック暗号「Hierocrypt-３」の設定処理として実行する。

【００８０】

まず、行列Ｐ３２は以下のように定義される。

【００８１】

【数２２】

$$P32 = \begin{pmatrix} I4 & O4 & I4 & O4 \\ O4 & I4 & O4 & I4 \\ O4 & I4 & I4 & I4 \\ I4 & O4 & I4 & I4 \end{pmatrix}$$

【００８２】

また、行列Ｐ３２Ｉを、行列Ｐ３２の逆行列とする。次に、行列Ｍ５１、Ｍ５２、ＭＢ１、ＭＢ２を以下のように定義する。

【００８３】

【数２３】

$$M51 = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

$$M52 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

$$MB1 = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

$$MB2 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

【００８４】

さらに、行列Ｍ５１、Ｍ５２、ＭＢ１、ＭＢ２を用いて、以下のように行列Ｍ５、ＭＢを定義する。

【００８５】

【数２４】

$$M5 = \begin{pmatrix} M51 & O4 & O4 & O4 \\ O4 & M52 & O4 & O4 \\ O4 & O4 & M51 & O4 \\ O4 & O4 & O4 & M52 \end{pmatrix}$$

$$MB = \begin{pmatrix} MB1 & O4 & O4 & O4 \\ O4 & MB2 & O4 & O4 \\ O4 & O4 & MB1 & O4 \\ O4 & O4 & O4 & MB2 \end{pmatrix}$$

【００８６】

次に、ラウンド依存定数ベクトルＧｉ（（ｉ＝０．．．９）を以下のように定義する。

【００８７】

【数２５】

$$G0 = (h11, h12, h13, h14, h01, h02, h03, h04, 0, 0, 0, 0, 0, 0, 0, 0)$$
$$G1 = (h21, h22, h23, h24, h31, h32, h33, h34, 0, 0, 0, 0, 0, 0, 0, 0)$$
$$G2 = (h31, h32, h33, h34, h01, h02, h03, h04, 0, 0, 0, 0, 0, 0, 0, 0)$$
$$G3 = (h11, h12, h13, h14, h31, h32, h33, h34, 0, 0, 0, 0, 0, 0, 0, 0)$$
$$G4 = (h21, h22, h23, h24, h11, h12, h13, h14, 0, 0, 0, 0, 0, 0, 0, 0)$$
$$G5 = (h01, h02, h03, h04, h21, h22, h23, h24, 0, 0, 0, 0, 0, 0, 0, 0)$$
$$G6 = (h01, h02, h03, h04, h21, h22, h23, h24, 0, 0, 0, 0, 0, 0, 0, 0)$$
$$G7 = (h21, h22, h23, h24, h11, h12, h13, h14, 0, 0, 0, 0, 0, 0, 0, 0)$$
$$G8 = (h11, h12, h13, h14, h31, h32, h33, h34, 0, 0, 0, 0, 0, 0, 0, 0)$$
$$G9 = (h31, h32, h33, h34, h01, h02, h03, h04, 0, 0, 0, 0, 0, 0, 0, 0)$$

【００８８】

なお、上式で用いられている定数を要素とするベクトルＨＨは、先に［暗号強度指標算出処理具体例２］において説明したと同一である。

【００８９】

次に、鍵スケジュール部の初期値の右半分から成るベクトルＺＺを、以下のように定義する。

【００９０】

【数２６】

ZZ=(z31,z32,z33,z34,z35,z36,z37,z38,z41,z42,z43,z44,z45,z46,z47,z48)

【００９１】

これらを用いて、共通鍵暗号アルゴリズムHierocrypt-３の鍵スケジュール部の右半分は、以下のように表せる。なお、演算子＋は、ガロア体ＧＦ（２）上の加法演算子である。

【００９２】

【数２７】

Ｚ０Ｍ５＊ＺＺ＋Ｇ０

Ｗ０＝Ｐ３２＊Ｚ０

Ｚ１＝Ｍ５＊Ｗ０＋Ｇ１

Ｗ１＝Ｐ３２＊Ｚ１

Ｚ２＝Ｍ５＊Ｗ１＋Ｇ２

Ｗ２＝Ｐ３２＊Ｚ２

Ｚ３＝Ｍ５＊Ｗ２＋Ｇ３

Ｗ３＝Ｐ３２＊Ｚ３

Ｚ４＝Ｍ５＊Ｗ３＋Ｇ４

Ｗ４＝Ｐ３２＊Ｚ４

Ｚ５＝Ｍ５＊Ｗ４＋Ｇ５

Ｗ６＝ＭＢ＊（Ｚ５＋Ｇ６）

Ｚ６＝Ｐ３２Ｉ＊Ｗ６

Ｗ７＝ＭＢ＊（Ｚ６＋Ｇ７）

Ｚ７＝Ｐ３２Ｉ＊Ｗ７

Ｗ８＝ＭＢ＊（Ｚ７＋Ｇ８）

Ｚ８＝Ｐ３２Ｉ＊Ｗ８

Ｗ９＝ＭＢ＊（Ｚ８＋Ｇ９）

Ｚ９＝Ｐ３２Ｉ＊Ｗ９

【００９３】

ここで、Z0,Z1,Z2,Z3,Z4,Z5,Z6,Z7,Z8,Z9,W0,W1,W2,W3,W5,W6,W7,W8,W9は、鍵スケジュール部の中間値の右半分を表す。

【００９４】

次に、これらの中間値を、下式、

【００９５】

【数２８】

$Zn = Zn_3 || ZN_4$

$Wn = Wn_1 || WN_2$

【００９６】

のように分割して表現する。但し記号“||”は、ベクトルの連結を表す。

【００９７】

次に、各ラウンドの非線形変換部出力を、V0,V1,V2,V3,V4,V5,V6,V7,V8,V9とする。

但し、各々は、下記に示す８つの要素から成るベクトルである。

【００９８】

【数２９】

V0＝(v01,v02,v03,v04,v05,v06,v07,v08)

V1＝(v11,v12,v13,v14,v15,v16,v17,v18)

V2＝(v21,v22,v23,v24,v25,v26,v27,v28)

V3＝(v31,v32,v33,v34,v35,v36,v37,v38)

V4＝(v41,v42,v43,v44,v45,v46,v47,v48)

V5＝(v51,v52,v53,v54,v55,v56,v57,v58)

V6＝(v61,v62,v63,v64,v65,v66,v67,v68)

V7＝(v71,v72,v73,v74,v75,v76,v77,v78)

V8＝(v81,v82,v83,v84,v85,v86,v87,v88)

V9＝(v91,v92,v93,v94,v95,v96,v97,v98)

【００９９】

ここで、ベクトルZ_1、Z_2を下記のように設定する。

【０１００】

【数３０】

Z_1＝(z11,z12,z13,z14,z15,z16,z17,z18)

$Z_2=(z21,z22,z23,z24,z25,z26,z27,z28)$

【０１０１】

上記のように、ベクトルZ_1、Z_2を設定すると、Hierocrypt-３の鍵スケジュール部の左半分は、以下のように表せる。

【０１０２】

【数３１】

$$Z0_1=Z_2$$
$$Z0_2=Z_1+V0$$
$$Z1_1=Z0_2$$
$$Z1_2=Z0_1+V1$$
$$Z2_1=Z1_2$$
$$Z2_2=Z1_1+V2$$
$$Z3_1=Z2_2$$
$$Z3_2=Z2_1+V3$$
$$Z4_1=Z3_2$$
$$Z4_2=Z3_1+V4$$
$$Z5_1=Z4_2$$
$$Z5_2=Z4_1+V5$$
$$Z6_1=Z5_2+V6$$
$$Z6_2=Z5_1$$
$$Z7_1=Z6_2+V7$$
$$Z7_2=Z6_1$$
$$Z8_1=Z7_2+V8$$
$$Z8_2=Z7_1$$
$$Z9_1=Z8_2+V9$$
$$Z9_2=Z8_1$$

【０１０３】

ここで、$Z0_1$, $Z0_2$, $Z1_1$, $Z1_2$, $Z2_1$, $Z2_2$, $Z3_1$, $Z3_2$, $Z4_1$, $Z4_2$, $Z5_1$, $Z5_2$, $Z6_1$, $Z6_2$, $Z7_1$, $Z7_2$, $Z8_1$, $Z8_2$, $Z9_1$,

$Z9_2$は、鍵スケジュール部の中間値の左半分を表す。こうして得られた中間値を用いて、ラウンド鍵$K1_1$，$K1_2$，$K1_3$，$K1_4$，$K2_1$，￥ｃｄｏｔｓ，$K9_1$，$K9_2$＄は、以下のように表せる。

【０１０４】

【数３２】

$$K1_1=Z0_1+V1$$
$$K1_2=Z1_3+V1$$
$$K1_3=Z1_4+V1$$
$$K1_4=Z0_2+Z1_4$$
$$K2_1=Z1_1+V2$$
$$K2_2=Z2_3+V2$$
$$K2_3=Z2_4+V2$$
$$K2_4=Z1_2+Z2_4$$
$$K3_1=Z2_1+V3$$
$$K3_2=Z3_3+V3$$
$$K3_3=Z3_4+V3$$
$$K3_4=Z2_2+Z3_4$$
$$K4_1=Z3_1+V4$$
$$K4_2=Z4_3+V4$$
$$K4_3=Z4_4+V4$$
$$K4_4=Z3_2+Z4_4$$
$$K5_1=Z4_1+V5$$
$$K5_2=Z5_3+V5$$
$$K5_3=Z5_4+V5$$
$$K5_4=Z4_2+Z5_4$$
$$K6_1=Z6_1+Z5_3$$
$$K6_2=W6_1+V6$$
$$K6_3=W6_2+V6$$
$$K6_4=Z5_1+W6_2$$

$K7_1=Z7_1+Z6_3$

$K7_2=W7_1+V7$

$K7_3=W7_2+V7$

$K7_4=Z6_1+W7_2$

$K8_1=Z8_1+Z7_3$

$K8_2=W8_1+V8$

$K8_3=W8_2+V8$

$K8_4=Z7_1+W8_2$

$K9_1=Z9_1+Z8_3$

$K9_2=W9_1+V9$

$K9_3=W9_2+V9$

$K9_4=Z8_1+W9_2$

【０１０５】

なお、$K1_1$，$K1_2$，$K1_3$，$K1_4$，$K2_1$，．．．，$K9_1$，$K9_2$は、８つの要素成るベクトルである。

【０１０６】

次に、図１に示すステップＳ１０２の中間変数消去処理ステップについて説明する。上述の８つの要素から成るベクトル$K1_1$，$K1_2$，$K1_3$，$K1_4$，$K2_1$，．．．，$K9_1$，$K9_2$について、実際に各値を代入して計算すると、以下のような式が得られる。

【０１０７】

【数３３】

$$K1_1 = \begin{pmatrix} v11 + z21 \\ v12 + z22 \\ v13 + z23 \\ v14 + z24 \\ v15 + z25 \\ v16 + z26 \\ v17 + z27 \\ v18 + z28 \end{pmatrix}$$

$$K1_2 = \begin{pmatrix} h11 + h21 + h13 + v11 + z32 + z42 \\ h11 + h12 + h22 + h14 + v12 + z33 + z43 \\ h11 + h12 + h13 + h23 + v13 + z31 + z41 + z34 + z44 \\ h12 + h14 + h24 + v14 + z31 + z41 \\ h01 + h02 + h03 + h04 + h31 + v15 + z36 + z46 + z38 + z48 \\ h02 + h03 + h04 + h32 + v16 + z35 + z45 + z37 + z47 \\ h03 + h04 + h33 + v17 + z35 + z36 + z45 + z46 + z38 + z48 \\ h01 + h02 + h03 + h34 + v18 + z35 + z45 + z37 + z38 + z47 + z48 \end{pmatrix}$$

$$K1_3 = \begin{pmatrix} h01+h03+v11+z42+z35+z36+z45+z46 \\ h01+h02+h04+v12+z43+z36+z37+z46+z47 \\ h01+h02+h03+v13+z41+z35+z44+z45+z37+z38+z47+z48 \\ h02+h04+v14+z41+z35+z45+z38+z48 \\ h11+h12+h13+h14+v15+z31+z32+z41+z42+z46+z48 \\ h12+h13+h14+v16+z32+z33+z42+z43+z45+z47 \\ h13+h14+v17+z31+z41+z33+z34+z43+z44+z45+z46+z48 \\ h11+h12+h13+z31+v18+z41+z34+z44+z45+z47+z48 \end{pmatrix}$$

$$K1_4 = \begin{pmatrix} h01+h03+v01+z11+z42+z35+z36+z45+z46 \\ h01+h02+h04+v02+z12+z43+z36+z37+z46+z47 \\ h01+h02+h03+v03+z13+z41+z35+z44+z45+z37+z38+z47+z48 \\ h02+h04+v04+z14+z41+z35+z45+z38+z48 \\ h11+h12+h13+h14+v05+z31+z32+z41+z15+z42+z46+z48 \\ h12+h13+h14+v06+z32+z33+z42+z16+z43+z45+z47 \\ h13+h14+v07+z31+z41+z33+z34+z43+z17+z44+z45+z46+z48 \\ h11+h12+h13+v08+z31+z41+z34+z44+z18+z45+z47+z48 \end{pmatrix}$$

$$K2_1 = \begin{pmatrix} v01+v21+z11 \\ v02+v22+z12 \\ v03+v23+z13 \\ v04+v24+z14 \\ v05+v25+z15 \\ v06+v26+z16 \\ v07+v27+z17 \\ v08+v28+z18 \end{pmatrix}$$

$$K2_2 = \begin{pmatrix} h02+h12+h21+h31+h23+v21+z31+z32+z34+z36+z37+z46+z38 \\ +z47+z48 \\ h03+h21+h13+h22+h32+h24+v22+z31+z32+z33+z37+z38+z47 \\ +z48 \\ h01+h11+h21+h04+h22+h14+h23+h33+v23+z31+z32+z33+z34 \\ +z38+z48 \\ h01+h11+h22+h24+h34+v24+z31+z33+z35+z36+z45+z37+z46 \\ +z38+z47+z48 \\ h01+h02+h12+h04+h31+h14+h32+h33+h34+v25+z31+z41+z35 \\ +z38 \\ h01+h02+h11+h03+h13+h32+h33+h34+v26+z32+z42+z35+z36 \\ h01+h02+h11+h03+h12+h04+h14+h33+h34+v27+z33+z43+z36 \\ +z37 \\ h01+h11+h03+h13+h31+h14+h32+h33+v28+z34+z44+z37 \end{pmatrix}$$

$$K2_3 = \begin{pmatrix} h01+h11+h12+h31+h33+v21+z32+z41+z33+z34+z43+z35+z36 \\ +z37+z46+z38+z47+z48 \\ h02+h12+h13+h31+h32+h34+v22+z41+z33+z42+z34+z44+z36 \\ +z37+z38+z47+z48 \\ h11+h03+h13+h31+h14+h32+h33+v23+z41+z42+z34+z43+z37 \\ +z38+z48 \\ h11+h04+h14+h32+h34+v24+z31+z32+z33+z42+z34+z35+z44 \\ +z36+z45+z37+z46+z47+z48 \\ h01+h02+h11+h21+h22+h14+h23+h24+v25+z31+z32+z41+z33 \\ +z34+z35+z48 \\ h02+h11+h03+h12+h22+h23+h24+v26+z32+z33+z42+z34+z36 \\ +z45 \\ h01+h03+h12+h04+h13+h23+h24+v27+z33+z34+z43+z37+z46 \\ h01+h21+h04+h13+h22+h23+z31+z32+v28+z33+z44+z38+z47 \\ +z48 \end{pmatrix}$$

$$K2_4 = \begin{pmatrix} h01+h11+h12+h31+h33+v11+z21+z32+z41+z33+z34+z43+z35 \\ +z36+z37+z46+z38+z47+z48 \\ h02+h12+h13+h31+h32+h34+v12+z22+z41+z33+z42+z34+z44 \\ +z36+z37+z38+z47+z48 \\ h11+h03+h13+h31+h14+h32+h33+v13+z23+z41+z42+z34+z43 \\ +z37+z38+z48 \\ h11+h04+h14+h32+h34+v14+z31+z32+z24+z33+z42+z34+z35 \\ +z44+z36+z45+z37+z46+z47+z48 \\ h01+h02+h11+h21+h22+h14+h23+h24+v15+z31+z32+z41+z33 \\ +z25+z34+z35+z48 \\ h02+h11+h03+h12+h22+h23+h24+v16+z32+z33+z42+z34+z26 \\ +z36+z45 \\ h01+h03+h12+h04+h13+h23+h24+v17+z33+z34+z43+z27+z37 \\ +z46 \\ h01+h21+h04+h13+h22+h23+z31+v18+z32+z33+z44+z28+z38 \\ +z47+z48 \end{pmatrix}$$

$$K3_1 = \begin{pmatrix} v11+v31+z21 \\ v12+v32+z22 \\ v13+v33+z23 \\ v14+v34+z24 \\ v15+v35+z25 \\ v16+v36+z26 \\ v17+v37+z27 \\ v18+v38+z28 \end{pmatrix}$$

$$K3_2 = \begin{pmatrix} h02+h03+h04+h13+h22+h31+h32+h33+v31+z32+z42+z35+z37 \\ h11+h03+h04+h31+h14+h23+h32+h33+h34+v32+z33+z43+z35 \\ +z36+z38 \\ h11+h12+h21+h04+h32+h24+h33+h34+v33+z31+z41+z34+z35 \\ +z44+z36+z37 \\ h01+h02+h03+h12+h21+h04+h31+h32+h34+v34+z31+z41+z36 \\ +z38 \\ h01+h02+h11+h03+h22+h31+h32+h24+h34+v35+z31+z33+z35 \\ +z36+z45+z37+z46+z47 \\ h01+h02+h03+h12+h21+h04+h31+h23+h32+h33+z31+v36+z32 \\ +z34+z35+z36+z45+z37+z46+z38+z47+z48 \\ h02+h03+h21+h04+h13+h22+h31+h32+h24+h33+h34+z31+z32 \\ +v37+z33+z36+z37+z46+z38+z47+z48 \\ h01+h02+h21+h04+h31+h14+h23+h24+h33+z32+v38+z34+z35 \\ +z36+z45+z46+z38+z48 \end{pmatrix}$$

$$K3_3 = \begin{pmatrix} h01+h02+h03+h21+h04+h22+h31+v31+z42+z35+z38+z47+z48 \\ h02+h03+h04+h22+h23+h32+v32+z43+z35+z36+z48 \\ h03+h21+h04+h23+h24+h33+v33+z41+z44+z36+z45+z37 \\ h01+h02+h03+h21+h24+h34+v34+z41+z37+z46+z47+z48 \\ h11+h12+h21+h13+h24+h33+h34+v35+z31+z34+z43+z44+z45 \\ +z46+z47 \\ h11+h12+h21+h13+h22+h14+h34+z31+v36+z32+z44+z45+z46 \\ +z47+z48 \\ h12+h13+h22+h31+h14+h23+z32+z41+v37+z33+z46+z47+z48 \\ h11+h12+h14+h23+h32+h33+h34+z33+z42+v38+z43+z44+z45 \\ +z46+z48 \end{pmatrix}$$

$$K3_4 = \begin{pmatrix} h01+h02+h03+h21+h04+h22+h31+v01+v21+z11+z42+z35+z38 \\ +z47+z48 \\ h02+h03+h04+h22+h23+h32+v02+v22+z12+z43+z35+z36+z48 \\ h03+h21+h04+h23+h24+h33+v03+v23+z13+z41+z44+z36+z45 \\ +z37 \\ h01+h02+h03+h21+h24+h34+v04+v24+z14+z41+z37+z46+z47 \\ +z48 \\ h11+h12+h21+h13+h24+h33+h34+v05+v25+z31+z15+z34+z43 \\ +z44+z45+z46+z47 \\ h11+h12+h21+h13+h22+h14+h34+v06+v26+z31+z32+z16+z44 \\ +z45+z46+z47+z48 \\ h12+h13+h22+h31+h14+h23+v07+v27+z32+z41+z33+z17+z46 \\ +z47+z48 \\ h11+h12+h14+h23+h32+h33+h34+v08+v28+z33+z42+z43+z44 \\ +z18+z45+z46+z48 \end{pmatrix}$$

$$K4_1 = \begin{pmatrix} v01+v21+v41+z11 \\ v02+v22+v42+z12 \\ v03+v23+v43+z13 \\ v04+v24+v44+z14 \\ v05+v25+v45+z15 \\ v06+v26+v46+z16 \\ v07+v27+v47+z17 \\ v08+v28+v48+z18 \end{pmatrix}$$

$$K4_2 = \begin{pmatrix} h01+h11+h03+h12+h13+h23+h33+h34+v41+z31+z32+z34+z35+z45 \\ +z37+z38+z47+z48 \\ h01+h02+h11+h12+h21+h04+h13+h14+h24+h34+v42+z31+z32+z33 \\ +z36+z46+z38+z48 \\ h01+h02+h03+h12+h21+h13+h22+h31+h14+v43+z31+z32+z33+z34 \\ +z35+z45+z37+z47 \\ h02+h11+h12+h04+h22+h14+h32+h33+h34+v44+z31+z33+z36+z37 \\ +z46+z47 \\ h01+h11+h03+h12+h21+h04+h31+h33+h34+z31+v45+z32+z41+z42 \\ +z34+z35+z44+z37+z38 \\ h02+h12+h04+h13+h22+h32+h34+z31+z32+z41+v46+z33+z42+z43 \\ +z36+z38 \\ h01+h11+h03+h13+h31+h14+h23+h33+z31+z32+z41+z33+z42+v47 \\ +z34+z43+z35+z44+z37 \\ h02+h11+h03+h14+h32+h24+h33+z31+z41+z33+z43+v48+z36+z37 \end{pmatrix}$$

$$K4_3 = \begin{pmatrix} h02+h04+h13+h14+h33+h34+v41+z31+z33+z42+z34+z43+z36+z45 \\ +z37+z47+z48 \\ h01+h03+h14+h34+v42+z32+z41+z34+z43+z35+z44+z37+z46+z38 \\ +z48 \\ h01+h02+h11+h04+h31+v43+z31+z33+z42+z44+z36+z45+z38+z47 \\ h01+h03+h12+h04+h13+h14+h32+h33+h34+v44+z32+z41+z33+z42 \\ +z35+z36+z46+z47 \\ h01+h02+h11+h03+h21+h04+h22+h31+h23+h34+v45+z32+z41+z33 \\ +z42+z35+z44+z36+z46+z38+z47 \\ h02+h03+h12+h21+h04+h22+h31+h23+h32+h24+z31+z41+v46+z33 \\ +z42+z34+z43+z35+z36+z45+z37+z47+z48 \\ h03+h04+h13+h22+h23+h32+h24+h33+z32+z41+z42+v47+z34+z43 \\ +z35+z44+z36+z37+z46+z38+z48 \\ h01+h02+h03+h21+h22+h14+h24+h33+z31+z32+z41+z43+v48+z35 \\ +z45+z37+z46 \end{pmatrix}$$

$$K4_4 = \begin{pmatrix} h02+h04+h13+h14+h33+h34+v11+v31+z21+z31+z33+z42+z34+z43 \\ +z36+z45+z37+z47+z48 \\ h01+h03+h14+h34+v12+v32+z22+z32+z41+z34+z43+z35+z44+z37 \\ +z46+z38+z48 \\ h01+h02+h11+h04+h31+v13+v33+z31+z23+z33+z42+z44+z36+z45 \\ +z38+z47 \\ h01+h03+h12+h04+h13+h14+h32+h33+h34+v14+v34+z32+z41+z24 \\ +z33+z42+z35+z36+z46+z47 \\ h01+h02+h11+h03+h21+h04+h22+h31+h23+h34+v15+v35+z32+z41 \\ +z33+z42+z25+z35+z44+z36+z46+z38+z47 \\ h02+h03+h12+h21+h04+h22+h31+h23+h32+h24+v16+z31+v36+z41 \\ +z33+z42+z34+z43+z26+z35+z36+z45+z37+z47+z48 \\ h03+h04+h13+h22+h23+h32+h24+h33+v17+z32+z41+v37+z42+z34 \\ +z43+z35+z44+z27+z36+z37+z46+z38+z48 \\ h01+h02+h03+h21+h22+h14+h24+h33+z31+v18+z32+z41+v38+z43 \\ +z35+z45+z28+z37+z46 \end{pmatrix}$$

$$K5_1 = \begin{pmatrix} v11+v31+v51+z21 \\ v12+v32+v52+z22 \\ v13+v33+v53+z23 \\ v14+v34+v54+z24 \\ v15+v35+v55+z25 \\ v16+v36+v56+z26 \\ v17+v37+v57+z27 \\ v18+v38+v58+z28 \end{pmatrix}$$

$$K5_2 = \begin{pmatrix} h02+h21+h13+h22+h23+v51+z33+z34+z43+z44+z37 \\ h11+h03+h21+h22+h14+h23+h24+v52+z34+z35+z44+z38 \\ h01+h11+h12+h04+h22+h23+h24+v53+z31+z41+z35+z36 \\ h01+h12+h21+h22+h24+v54+z32+z33+z42+z34+z43+z44+z36 \\ h02+h03+h12+h21+h04+h13+h22+h14+h33+h34+v55+z33+z36+z46 \\ h03+h04+h13+h22+h14+h23+h34+z31+v56+z34+z37+z47 \\ h21+h04+h31+h14+h23+h24+z31+z32+v57+z35+z45+z38+z48 \\ h01+h02+h11+h03+h12+h21+h04+h13+h14+h32+h24+h33+h34+z32 \\ +z35+v58+z45 \end{pmatrix}$$

$$K5_3 = \begin{pmatrix} h02+h12+h04+h13+h23+h32+h24+h34+v51+z43+z44+z47 \\ h01+h11+h03+h13+h31+h14+h24+h33+v52+z44+z45+z48 \\ h01+h02+h12+h21+h04+h31+h14+h32+h34+v53+z41+z45+z46 \\ h01+h11+h03+h12+h04+h22+h31+h23+h24+h33+h34+v54+z42+z43 \\ +z44+z46 \\ h11+h21+h14+h34+v55+z43+z46 \\ h11+h12+h22+h31+z41+v56+z44+z47 \\ h12+h13+h23+h32+z41+z42+v57+z45+z48 \\ h13+h24+h33+h34+z42+v58+z45 \end{pmatrix}$$

$$K5_4 = \begin{pmatrix} h02+h12+h04+h13+h23+h32+h24+h34+v01+v21+v41+z11+z43 \\ +z44+z47 \\ h01+h11+h03+h13+h31+h14+h24+h33+v02+v22+v42+z12+z44 \\ +z45+z48 \\ h01+h02+h12+h21+h04+h31+h14+h32+h34+v03+v23+v43+z13 \\ +z41+z45+z46 \\ h01+h11+h03+h12+h04+h22+h31+h23+h24+h33+h34+v04+v24 \\ +v44+z14+z42+z43+z44+z46 \\ h11+h21+h14+h34+v05+v25+v45+z15+z43+z46 \\ h11+h12+h22+h31+v06+v26+z41+v46+z16+z44+z47 \\ h12+h13+h23+h32+v07+v27+z41+z42+v47+z17+z45+z48 \\ h13+h24+h33+h34+v08+v28+z42+v48+z18+z45 \end{pmatrix}$$

$$K6_1 = \begin{pmatrix} h02+h21+h13+h22+h23+v11+v31+v51+v61+z21+z33+z34+z43 \\ +z44+z37 \\ h11+h03+h21+h22+h14+h23+h24+v12+v32+v52+v62+z22+z34 \\ +z35+z44+z38 \\ h01+h11+h12+h04+h22+h23+h24+v13+v33+v53+z31+v63+z23 \\ +z41+z35+z36 \\ h01+h12+h21+h22+h24+v14+v34+v54+z32+v64+z24+z33+z42 \\ +z34+z43+z44+z36 \\ h02+h03+h12+h21+h04+h13+h22+h14+h33+h34+v15+v35+v55 \\ +z33+v65+z25+z36+z46 \\ h03+h04+h13+h22+h14+h23+h34+v16+z31+v36+v56+z34+v66 \\ +z26+z37+z47 \\ h21+h04+h31+h14+h23+h24+v17+z31+z32+v37+v57+z35+v67 \\ +z27+z45+z38+z48 \\ h01+h02+h11+h03+h12+h21+h04+h13+h14+h32+h24+h33+h34 \\ +v18+z32+v38+z35+v58+z45+v68+z28 \end{pmatrix}$$

$$K6_2 = \begin{pmatrix} h01+h02+h11+h03+h12+h04+h14+h23+v61+z32+z33+z42+z43 \\ +z35+z36+z38 \\ h02+h11+h03+h12+h21+h04+h13+h24+v62+z31+z41+z33+z34 \\ +z43+z35+z44+z36+z37 \\ h11+h03+h12+h21+h04+h13+h22+h14+v63+z32+z42+z34+z35 \\ +z44+z36+z37+z38 \\ h01+h02+h11+h03+h13+h22+z31+z32+z41+v64+z42+z35+z37 \\ h02+h12+h22+h23+h33+z31+z33+v65+z34+z36+z37+z46+z47 \\ h03+h21+h13+h31+h23+h24+h34+z32+z34+v66+z35+z45+z37 \\ +z38+z47+z48 \\ h01+h11+h04+h22+h31+h14+h32+h24+z31+z33+v67+z36+z46 \\ +z38+z48 \\ h01+h11+h21+h22+h32+z32+z33+z35+z36+z45+v68+z46 \end{pmatrix}$$

$$K6_3 = \begin{pmatrix} h12+h04+h13+h22+h14+h23+h34+v61+z42+z43+z45+z46+z48 \\ h01+h21+h13+h31+h14+h23+h24+v62+z41+z43+z44+z45+z46 \\ +z47 \\ h02+h22+h14+h32+h24+v63+z42+z44+z45+z46+z47+z48 \\ h11+h03+h12+h21+h04+h13+h22+h14+h33+h34+z41+v64+z42 \\ +z45+z47 \\ h12+h21+h22+h31+h14+h34+z41+v65+z43+z44+z46+z47 \\ h11+h13+h22+h31+h23+h32+z42+v66+z44+z45+z47+z48 \\ h11+h12+h21+h14+h23+h32+h24+h33+z41+z43+v67+z46+z48 \\ h11+h21+h13+h14+h24+h33+z42+z43+z45+v68+z46 \end{pmatrix}$$

$$K6_4 = \begin{pmatrix} h12+h04+h13+h22+h14+h23+h34+v01+v21+v41+z11+z42+z43 \\ +z45+z46+z48 \\ h01+h21+h13+h31+h14+h23+h24+v02+v22+v42+z12+z41+z43 \\ +z44+z45+z46+z47 \\ h02+h22+h14+h32+h24+v03+v23+v43+z13+z42+z44+z45+z46 \\ +z47+z48 \\ h11+h03+h12+h21+h04+h13+h22+h14+h33+h34+v04+v24+v44 \\ +z14+z41+z42+z45+z47 \\ h12+h21+h22+h31+h14+h34+v05+v25+v45+z41+z15+z43+z44 \\ +z46+z47 \\ h11+h13+h22+h31+h23+h32+v06+v26+v46+z42+z16+z44+z45 \\ +z47+z48 \\ h11+h12+h21+h14+h23+h32+h24+h33+v07+v27+z41+v47+z43 \\ +z17+z46+z48 \\ h11+h21+h13+h14+h24+h33+v08+v28+z42+z43+v48+z18+z45 \\ +z46 \end{pmatrix}$$

$$K7_1 = \begin{pmatrix} h01+h11+h03+h12+h13+h23+h33+h34+v01+v21+v41+z11+v71 \\ +z31+z32+z34+z35+z45+z37+z38+z47+z48 \\ h01+h02+h11+h12+h21+h04+h13+h14+h24+h34+v02+v22+v42 \\ +z12+z31+v72+z32+z33+z36+z46+z38+z48 \\ h01+h02+h03+h12+h21+h13+h22+h31+h14+v03+v23+v43+z13 \\ +z31+z32+v73+z33+z34+z35+z45+z37+z47 \\ h02+h11+h12+h04+h22+h14+h32+h33+h34+v04+v24+v44+z31 \\ +z14+z33+v74+z36+z37+z46+z47 \\ h01+h11+h03+h12+h21+h04+h31+h33+h34+v05+v25+z31+v45 \\ +z32+z41+z15+z42+z34+v75+z35+z44+z37+z38 \\ h02+h12+h04+h13+h22+h32+h34+v06+v26+z31+z32+z41+v46 \\ +z33+z42+z16+z43+v76+z36+z38 \\ h01+h11+h03+h13+h31+h14+h23+h33+v07+z31+v27+z32+z41 \\ +z33+z42+v47+z34+z43+z17+z35+z44+v77+z37 \\ h02+h11+h03+h14+h32+h24+h33+v08+z31+z41+v28+z33+z43 \\ +v48+z18+z36+z37+v78 \end{pmatrix}$$

$$K7_2 = \begin{pmatrix} h01+h21+h13+h32+h33+v71+z32+z37+z38+z47+z48 \\ h02+h11+h22+h31+h14+h33+h34+v72+z33+z38+z48 \\ h11+h03+h12+h23+h32+h34+z31+v73+z34+z35+z45 \\ h12+h04+h31+h32+h24+z31+v74+z36+z37+z46+z38+z47+z48 \\ h01+h02+h03+h12+h21+h13+h22+h31+h32+h33+z33+z34+z43 \\ +v75+z35+z44+z36+z37 \\ h01+h02+h11+h03+h04+h13+h22+h31+h14+h23+h32+h33+h34 \\ +z34+z35+z44+v76+z36+z37+z38 \\ h02+h03+h12+h21+h04+h14+h23+h32+h24+h33+h34+z31+z41 \\ +z36+v77+z37+z38 \\ h01+h02+h11+h12+h21+h04+h31+h32+h24+h34+z32+z33+z42 \\ +z34+z43+z35+z44+z36+v78+z38 \end{pmatrix}$$

$$K7_3 = \begin{pmatrix} h12+h04+h13+h32+h33+v71+z33+z42+z34+z43+z44+z36+z37 \\ +z38+z47+z48 \\ h01+h11+h13+h31+h14+h33+h34+v72+z34+z43+z44+z37+z38+z48 \\ h02+h12+h14+h32+h34+z31+v73+z44+z45+z38 \\ h11+h03+h12+h04+h31+h32+z32+z41+z33+z42+v74+z34+z43 \\ +z35+z44+z36+z37+z46+z38+z47+z48 \\ h01+h11+h12+h32+h24+h34+z31+z32+z34+z43+v75+z44+z45 \\ +z37+z46+z38+z48 \\ h02+h12+h21+h13+h31+h33+z31+z32+z33+z44+v76+z45+z46 \\ +z38+z47 \\ h11+h03+h13+h22+h31+h14+h32+h34+z31+z32+z41+z33+z34 \\ +z35+z45+v77+z46+z47+z48 \\ h11+h04+h31+h14+h23+h24+h33+h34+z31+z33+z42+z43+z44 \\ +z36+z45+z37+v78+z38+z47 \end{pmatrix}$$

$$K7_4 = \begin{pmatrix} h12+h04+h13+h32+h33+v11+v31+v51+v61+z21+z33+z42+z34+z43 \\ +z44+z36+z37+z38+z47+z48 \\ h01+h11+h13+h31+h14+h33+h34+v12+v32+v52+v62+z22+z34+z43 \\ +z44+z37+z38+z48 \\ h02+h12+h14+h32+h34+v13+v33+v53+z31+v63+z23+z44+z45+z38 \\ h11+h03+h12+h04+h31+h32+v14+v34+v54+z32+z41+v64+z24+z33 \\ +z42+z34+z43+z35+z44+z36+z37+z46+z38+z47+z48 \\ h01+h11+h12+h32+h24+h34+v15+v35+z31+z32+v55+v65+z25+z34 \\ +z43+z44+z45+z37+z46+z38+z48 \\ h02+h12+h21+h13+h31+h33+v16+z31+v36+z32+z33+v56+v66+z26 \\ +z44+z45+z46+z38+z47 \\ h11+h03+h13+h22+h31+h14+h32+h34+v17+z31+z32+z41+v37+z33 \\ +z34+v57+z35+v67+z27+z45+z46+z47+z48 \\ h11+h04+h31+h14+h23+h24+h33+h34+z31+v18+z33+z42+v38+z43 \\ +z44+v58+z36+z45+v68+z28+z37+z38+z47 \end{pmatrix}$$

$$K8_1 = \begin{pmatrix} h02+h03+h04+h13+h22+h31+h32+h33+v11+v31+v51+v61+z21+v81 \\ +z32+z42+z35+z37 \\ h11+h03+h04+h31+h14+h23+h32+h33+h34+v12+v32+v52+v62+z22 \\ +v82+z33+z43+z35+z36+z38 \\ h11+h12+h21+h04+h32+h24+h33+h34+v13+v33+v53+z31+v63+z23 \\ +z41+v83+z34+z35+z44+z36+z37 \\ h01+h02+h03+h12+h21+h04+h31+h32+h34+v14+v34+z31+v54+z41 \\ +v64+z24+v84+z36+z38 \\ h01+h02+h11+h03+h22+h31+h32+h24+h34+v15+v35+z31+v55+z33 \\ +v65+z25+z35+v85+z36+z45+z37+z46+z47 \\ h01+h02+h03+h12+h21+h04+h31+h23+h32+h33+v16+z31+v36+z32 \\ +v56+z34+v66+z26+z35+z36+z45+v86+z37+z46+z38+z47+z48 \\ h02+h03+h21+h04+h13+h22+h31+h32+h24+h33+h34+v17+z31+z32 \\ +v37+z33+v57+v67+z27+z36+z37+z46+v87+z38+z47+z48 \\ h01+h02+h21+h04+h31+h14+h23+h24+h33+v18+z32+v38+z34+z35 \\ +v58+z36+z45+v68+z28+z46+z38+v88+z48 \end{pmatrix}$$

$$K8_2 = \begin{pmatrix} h01+h02+h11+h21+h23+h33+z31+v81+z41+z33+z43+z35 \\ h02+h03+h12+h21+h22+h31+h24+h34+z31+z32+z41+v82+z42+z34 \\ +z44+z36 \\ h01+h03+h21+h04+h13+h22+h31+h23+h32+z31+z32+z41+z33+z42 \\ +v83+z43+z37 \\ h01+h04+h22+h14+h32+h24+z32+z42+z34+v84+z44+z38 \\ h11+h12+h21+h04+h22+h31+h23+h32+h24+h33+h34+z32+z33+z34 \\ +v85+z38+z48 \\ h01+h12+h13+h22+h23+h32+h24+h33+h34+z33+z34+z35+z45+v86 \\ h02+h11+h13+h14+h23+h24+h33+h34+z34+z36+z46+v87 \\ h11+h03+h21+h04+h22+h31+h14+h23+h32+h33+z31+z32+z33+z34 \\ +z37+z38+z47+v88+z48 \end{pmatrix}$$

$$K8_3 = \begin{pmatrix} h01+h21+h04+h22+h23+h32+h24+h34+v81+z41+z43+z35+z36 \\ +z37+z46+z47 \\ h01+h02+h22+h31+h23+h24+h33+z41+v82+z42+z35+z44+z36 \\ +z45+z37+z38+z47+z48 \\ h02+h03+h31+h23+h32+h24+h34+z41+z42+v83+z43+z36+z37 \\ +z46+z38+z48 \\ h03+h21+h22+h31+h23+h33+h34+z42+v84+z35+z44+z36+z45 \\ +z46+z38 \\ h22+h14+h24+h33+z32+z34+z43+v85+z48 \\ h11+h21+h31+h23+h34+z31+z41+z33+z44+z45+v86 \\ h12+h21+h22+h31+h32+h24+z31+z32+z41+z42+z34+z46+v87 \\ h21+h13+h14+h23+h32+h24+z31+z33+z42+z34+z47+v88+z48 \end{pmatrix}$$

$$K8_4 = \begin{pmatrix} h01+h21+h04+h22+h23+h32+h24+h34+v01+v21+v41+z11+v71 \\ +z41+z43+z35+z36+z37+z46+z47 \\ h01+h02+h22+h31+h23+h24+h33+v02+v22+v42+z12+v72+z41 \\ +z42+z35+z44+z36+z45+z37+z38+z47+z48 \\ h02+h03+h31+h23+h32+h24+h34+v03+v23+v43+z13+z41+v73 \\ +z42+z43+z36+z37+z46+z38+z48 \\ h03+h21+h22+h31+h23+h33+h34+v04+v24+v44+z14+z42+v74 \\ +z35+z44+z36+z45+z46+z38 \\ h22+h14+h24+h33+v05+v25+v45+z32+z15+z34+z43+v75+z48 \\ h11+h21+h31+h23+h34+v06+v26+z31+z41+v46+z33+z16+z44 \\ +v76+z45 \\ h12+h21+h22+h31+h32+h24+v07+z31+v27+z32+z41+z42+v47 \\ +z34+z17+v77+z46 \\ h21+h13+h14+h23+h32+h24+v08+z31+v28+z33+z42+z34+v48 \\ +z18+v78+z47+z48 \end{pmatrix}$$

$$K9_1 = \begin{pmatrix} h02+h12+h21+h31+h23+v01+v21+v41+z11+v71+z31+z32+v91 \\ +z34+z36+z37+z46+z38+z47+z48 \\ h03+h21+h13+h22+h32+h24+v02+v22+v42+z12+z31+v72+z32 \\ +z33+v92+z37+z38+z47+z48 \\ h01+h11+h21+h04+h22+h14+h23+h33+v03+v23+v43+z13+z31 \\ +z32+v73+z33+z34+v93+z38+z48 \\ h01+h11+h22+h24+h34+v04+v24+v44+z31+z14+z33+v74+z35 \\ +v94+z36+z45+z37+z46+z38+z47+z48 \\ h01+h02+h12+h04+h31+h14+h32+h33+h34+v05+v25+z31+v45 \\ +z41+z15+v75+z35+v95+z38 \\ h01+h02+h11+h03+h13+h32+h33+h34+v06+v26+z32+v46+z42 \\ +z16+z35+v76+z36+v96 \\ h01+h02+h11+h03+h12+h04+h14+h33+h34+v07+v27+z33+v47 \\ +z43+z17+z36+v77+z37+v97 \\ h01+h11+h03+h13+h31+h14+h32+h33+v08+v28+z34+v48+z44 \\ +z18+z37+v78+v98 \end{pmatrix}$$

$$K9_2 = \begin{pmatrix} h01+h11+h03+h21+h13+z32+v91+z35+z36+z45+z46 \\ h01+h02+h11+h12+h04+h22+h14+z33+v92+z36+z37+z46+z47 \\ h01+h02+h11+h03+h12+h13+h23+z31+z34+v93+z35+z45+z37 \\ +z38+z47+z48 \\ h02+h12+h04+h14+h24+z31+z35+v94+z45+z38+z48 \\ h01+h02+h11+h03+h12+h04+h13+h31+h14+z31+z32+z41+z42 \\ +z36+v95+z38 \\ h02+h03+h12+h04+h13+h14+h32+z32+z33+z42+z43+z35+z37 \\ +v96 \\ h03+h04+h13+h14+h33+z31+z41+z33+z34+z43+z35+z44+z36 \\ +z38+v97 \\ h01+h02+h11+h03+h12+h13+h34+z31+z41+z34+z35+z44+z37 \\ +z38+v98 \end{pmatrix}$$

【０１０８】

次に、ステップＳ１０３の変数移項処理を実行する。上記Ｋ１$_1$，Ｋ１$_2$，Ｋ１$_3$，Ｋ１$_4$，Ｋ２$_1$，．．．，Ｋ９$_1$，Ｋ９$_2$の結果に基づいて、上記の連立線形方程式を変形し、右辺がｚｘｘ，ｖｘｘの項のみを含むように変形すると、以下のように表せる。

【０１０９】

【数３４】

$$k1_{11} = v11 + z21$$
$$k1_{12} = v12 + z22$$
$$k1_{13} = v13 + z23$$
$$k1_{14} = v14 + z24$$
$$k1_{15} = v15 + z25$$
$$k1_{16} = v16 + z26$$
$$k1_{17} = v17 + z27$$
$$k1_{18} = v18 + z28$$

$$h11 + h21 + h13 + k1_{21} = v11 + z32 + z42$$
$$h11 + h12 + h22 + h14 + k1_{22} = v12 + z33 + z43$$
$$h11 + h12 + h13 + h23 + k1_{23} = v13 + z31 + z41 + z34 + z44$$
$$h12 + h14 + h24 + k1_{24} = v14 + z31 + z41$$
$$h01 + h02 + h03 + h04 + h31 + k1_{25} = v15 + z36 + z46 + z38 + z48$$
$$h02 + h03 + h04 + h32 + k1_{26} = v16 + z35 + z45 + z37 + z47$$
$$h03 + h04 + h33 + k1_{27} = v17 + z35 + z36 + z45 + z46 + z38 + z48$$
$$h01 + h02 + h03 + h34 + k1_{28} = v18 + z35 + z45 + z37 + z38 + z47 + z48$$
$$h01 + h03 + k1_{31} = v11 + z42 + z35 + z36 + z45 + z46$$
$$h01 + h02 + h04 + k1_{32} = v12 + z43 + z36 + z37 + z46 + z47$$
$$h01 + h02 + h03 + k1_{33} = v13 + z41 + z35 + z44 + z45 + z37 + z38 + z47 + z48$$
$$h02 + h04 + k1_{34} = v14 + z41 + z35 + z45 + z38 + z48$$
$$h11 + h12 + h13 + h14 + k1_{35} = v15 + z31 + z32 + z41 + z42 + z46 + z48$$
$$h12 + h13 + h14 + k1_{36} = v16 + z32 + z33 + z42 + z43 + z45 + z47$$
$$h13 + h14 + k1_{37} = v17 + z31 + z41 + z33 + z34 + z43 + z44 + z45 + z46 + z48$$
$$h11 + h12 + h13 + z31 + k1_{38} = v18 + z41 + z34 + z44 + z45 + z47 + z48$$
$$h01 + h03 + k1_{41} = v01 + z11 + z42 + z35 + z36 + z45 + z46$$
$$h01 + h02 + h04 + k1_{42} = v02 + z12 + z43 + z36 + z37 + z46 + z47$$
$$h01 + h02 + h03 + k1_{43} = v03 + z13 + z41 + z35 + z44 + z45 + z37 + z38 + z47 + z48$$
$$h02 + h04 + k1_{44} = v04 + z14 + z41 + z35 + z45 + z38 + z48$$
$$h11 + h12 + h13 + h14 + k1_{45} = v05 + z31 + z32 + z41 + z15 + z42 + z46 + z48$$
$$h12 + h13 + h14 + k1_{46} = v06 + z32 + z33 + z42 + z16 + z43 + z45 + z47$$
$$h13 + h14 + k1_{47} = v07 + z31 + z41 + z33 + z34 + z43 + z17 + z44 + z45 + z46 + z48$$
$$h11 + h12 + h13 + k1_{48} = v08 + z31 + z41 + z34 + z44 + z18 + z45 + z47 + z48$$
$$k2_{11} = v01 + v21 + z11$$
$$k2_{12} = v02 + v22 + z12$$
$$k2_{13} = v03 + v23 + z13$$
$$k2_{14} = v04 + v24 + z14$$
$$k2_{15} = v05 + v25 + z15$$
$$k2_{16} = v06 + v26 + z16$$
$$k2_{17} = v07 + v27 + z17$$
$$k2_{18} = v08 + v28 + z18$$
$$h02 + h12 + h21 + h31 + h23 + k2_{21} = v21 + z31 + z32 + z34 + z36 + z37 + z46 + z38 + z47 + z48$$
$$h03 + h21 + h13 + h22 + h32 + h24 + k2_{22} = v22 + z31 + z32 + z33 + z37 + z38 + z47 + z48$$

$h01+h11+h21+h04+h22+h14+h23+h33+k2_{23}=v23+z31+z32+z33+z34+z38+z48$

$h01+h11+h22+h24+h34+k2_{24}=v24+z31+z33+z35+z36+z45+z37+z46+z38+z47+z48$

$h01+h02+h12+h04+h31+h14+h32+h33+h34+k2_{25}=v25+z31+z41+z35+z38$

$h01+h02+h11+h03+h13+h32+h33+h34+k2_{26}=v26+z32+z42+z35+z36$

$h01+h02+h11+h03+h12+h04+h14+h33+h34+k2_{27}=v27+z33+z43+z36+z37$

$h01+h11+h03+h13+h31+h14+h32+h33+k2_{28}=v28+z34+z44+z37$

$h01+h11+h12+h31+h33+k2_{31}=v21+z32+z41+z33+z34+z43+z35+z36+z37+z46+z38+z47+z48$

$h02+h12+h13+h31+h32+h34+k2_{32}=v22+z41+z33+z42+z34+z44+z36+z37+z38+z47+z48$

$h11+h03+h13+h31+h14+h32+h33+k2_{33}=v23+z41+z42+z34+z43+z37+z38+z48$

$h11+h04+h14+h32+h34+k2_{34}=v24+z31+z32+z33+z42+z34+z35+z44+z36+z45+z37+z46+z47+z48$

$h01+h02+h11+h21+h22+h14+h23+h24+k2_{35}=v25+z31+z32+z41+z33+z34+z35+z48$

$h02+h11+h03+h12+h22+h23+h24+k2_{36}=v26+z32+z33+z42+z34+z36+z45$

$h01+h03+h12+h04+h13+h23+h24+k2_{37}=v27+z33+z34+z43+z37+z46$

$h01+h21+h04+h13+h22+h23+z31+z32+k2_{38}=v28+z33+z44+z38+z47+z48$

$h01+h11+h12+h31+h33+k2_{41}=v11+z21+z32+z41+z33+z34+z43+z35+z36+z37+z46+z38+z47+z48$

$h02+h12+h13+h31+h32+h34+k2_{42}=v12+z22+z41+z33+z42+z34+z44+z36+z37+z38+z47+z48$

$h11+h03+h13+h31+h14+h32+h33+k2_{43}=v13+z23+z41+z42+z34+z43+z37+z38+z48$

$h11+h04+h14+h32+h34+k2_{44}=v14+z31+z32+z24+z33+z42+z34+z35+z44+z36+z45+z37+z46+z47+z48$

$h01+h02+h11+h21+h22+h14+h23+h24+k2_{45}=v15+z31+z32+z41+z33+z25+z34+z35+z48$

$h02+h11+h03+h12+h22+h23+h24+k2_{46}=v16+z32+z33+z42+z34+z26+z36+z45$

$h01 + h03 + h12 + h04 + h13 + h23 + h24 + k2_{47} = v17 + z33 + z34 + z43 + z27 + z37 + z46$

$h01 + h21 + h04 + h13 + h22 + h23 + z31 + k2_{48} = v18 + z32 + z33 + z44 + z28 + z38 + z47 + z48$

$k3_{11} = v11 + v31 + z21$

$k3_{12} = v12 + v32 + z22$

$k3_{13} = v13 + v33 + z23$

$k3_{14} = v14 + v34 + z24$

$k3_{15} = v15 + v35 + z25$

$k3_{16} = v16 + v36 + z26$

$k3_{17} = v17 + v37 + z27$

$k3_{18} = v18 + v38 + z28$

$h02 + h03 + h04 + h13 + h22 + h31 + h32 + h33 + k3_{21} = v31 + z32 + z42 + z35 + z37$

$h11 + h03 + h04 + h31 + h14 + h23 + h32 + h33 + h34 + k3_{22} = v32 + z33 + z43 + z35 + z36 + z38$

$h11 + h12 + h21 + h04 + h32 + h24 + h33 + h34 + k3_{23} = v33 + z31 + z41 + z34 + z35 + z44 + z36 + z37$

$h01 + h02 + h03 + h12 + h21 + h04 + h31 + h32 + h34 + k3_{24} = v34 + z31 + z41 + z36 + z38$

$h01 + h02 + h11 + h03 + h22 + h31 + h32 + h24 + h34 + k3_{25} = v35 + z31 + z33 + z35 + z36 + z45 + z37 + z46 + z47$

$h01 + h02 + h03 + h12 + h21 + h04 + h31 + h23 + h32 + h33 + z31 + k3_{26} = v36 + z32 + z34 + z35 + z36 + z45 + z37 + z46 + z38 + z47 + z48$

$h02 + h03 + h21 + h04 + h13 + h22 + h31 + h32 + h24 + h33 + h34 + z31 + z32 + k3_{27} = v37 + z33 + z36 + z37 + z46 + z38 + z47 + z48$

$h01 + h02 + h21 + h04 + h31 + h14 + h23 + h24 + h33 + z32 + k3_{28} = v38 + z34 + z35 + z36 + z45 + z46 + z38 + z48$

$h01 + h02 + h03 + h21 + h04 + h22 + h31 + k3_{31} = v31 + z42 + z35 + z38 + z47 + z48$

$h02 + h03 + h04 + h22 + h23 + h32 + k3_{32} = v32 + z43 + z35 + z36 + z48$

$h03 + h21 + h04 + h23 + h24 + h33 + k3_{33} = v33 + z41 + z44 + z36 + z45 + z37$

$h01 + h02 + h03 + h21 + h24 + h34 + k3_{34} = v34 + z41 + z37 + z46 + z47 + z48$

$h11 + h12 + h21 + h13 + h24 + h33 + h34 + k3_{35} = v35 + z31 + z34 + z43 + z44 + z45 + z46 + z47$

$h11 + h12 + h21 + h13 + h22 + h14 + h34 + z31 + k3_{36} = v36 + z32 + z44 + z45 + z46 + z47 + z48$

$h12 + h13 + h22 + h31 + h14 + h23 + z32 + z41 + k3_{37} = v37 + z33 + z46 + z47 + z48$

$$h11 + h12 + h14 + h23 + h32 + h33 + h34 + z33 + z42 + k3_{38} = v38 + z43 + z44 + z45 + z46 + z48$$

$$h01 + h02 + h03 + h21 + h04 + h22 + h31 + k3_{41} = v01 + v21 + z11 + z42 + z35 + z38 + z47 + z48$$

$$h02 + h03 + h04 + h22 + h23 + h32 + k3_{42} = v02 + v22 + z12 + z43 + z35 + z36 + z48$$

$$h03 + h21 + h04 + h23 + h24 + h33 + k3_{43} = v03 + v23 + z13 + z41 + z44 + z36 + z45 + z37$$

$$h01 + h02 + h03 + h21 + h24 + h34 + k3_{44} = v04 + v24 + z14 + z41 + z37 + z46 + z47 + z48$$

$$h11 + h12 + h21 + h13 + h24 + h33 + h34 + k3_{45} = v05 + v25 + z31 + z15 + z34 + z43 + z44 + z45 + z46 + z47$$

$$h11 + h12 + h21 + h13 + h22 + h14 + h34 + k3_{46} = v06 + v26 + z31 + z32 + z16 + z44 + z45 + z46 + z47 + z48$$

$$h12 + h13 + h22 + h31 + h14 + h23 + k3_{47} = v07 + v27 + z32 + z41 + z33 + z17 + z46 + z47 + z48$$

$$h11 + h12 + h14 + h23 + h32 + h33 + h34 + k3_{48} = v08 + v28 + z33 + z42 + z43 + z44 + z18 + z45 + z46 + z48$$

$$k4_{11} = v01 + v21 + v41 + z11$$

$$k4_{12} = v02 + v22 + v42 + z12$$

$$k4_{13} = v03 + v23 + v43 + z13$$

$$k4_{14} = v04 + v24 + v44 + z14$$

$$k4_{15} = v05 + v25 + v45 + z15$$

$$k4_{16} = v06 + v26 + v46 + z16$$

$$k4_{17} = v07 + v27 + v47 + z17$$

$$k4_{18} = v08 + v28 + v48 + z18$$

$$h01 + h11 + h03 + h12 + h13 + h23 + h33 + h34 + k4_{21} = v41 + z31 + z32 + z34 + z35 + z45 + z37 + z38 + z47 + z48$$

$$h01 + h02 + h11 + h12 + h21 + h04 + h13 + h14 + h24 + h34 + k4_{22} = v42 + z31 + z32 + z33 + z36 + z46 + z38 + z48$$

$$h01 + h02 + h03 + h12 + h21 + h13 + h22 + h31 + h14 + k4_{23} = v43 + z31 + z32 + z33 + z34 + z35 + z45 + z37 + z47$$

$$h02 + h11 + h12 + h04 + h22 + h14 + h32 + h33 + h34 + k4_{24} = v44 + z31 + z33 + z36 + z37 + z46 + z47$$

$$h01 + h11 + h03 + h12 + h21 + h04 + h31 + h33 + h34 + z31 + k4_{25} = v45 + z32 + z41 + z42 + z34 + z35 + z44 + z37 + z38$$

$$h02 + h12 + h04 + h13 + h22 + h32 + h34 + z31 + z32 + z41 + k4_{26} = v46 + z33 + z42 + z43 + z36 + z38$$

$$h01+h11+h03+h13+h31+h14+h23+h33+z31+z32+z41+z33+z42+k4_{27}=v47+z34+z43+z35+z44+z37$$

$$h02+h11+h03+h14+h32+h24+h33+z31+z41+z33+z43+k4_{28}=v48+z36+z37$$

$$h02+h04+h13+h14+h33+h34+k4_{31}=v41+z31+z33+z42+z34+z43+z36+z45+z37+z47+z48$$

$$h01+h03+h14+h34+k4_{32}=v42+z32+z41+z34+z43+z35+z44+z37+z46+z38+z48$$

$$h01+h02+h11+h04+h31+k4_{33}=v43+z31+z33+z42+z44+z36+z45+z38+z47$$

$$h01+h03+h12+h04+h13+h14+h32+h33+h34+k4_{34}=v44+z32+z41+z33+z42+z35+z36+z46+z47$$

$$h01+h02+h11+h03+h21+h04+h22+h31+h23+h34+k4_{35}=v45+z32+z41+z33+z42+z35+z44+z36+z46+z38+z47$$

$$h02+h03+h12+h21+h04+h22+h31+h23+h32+h24+z31+z41+k4_{36}=v46+z33+z42+z34+z43+z35+z36+z45+z37+z47+z48$$

$$h03+h04+h13+h22+h23+h32+h24+h33+z32+z41+z42+k4_{37}=v47+z34+z43+z35+z44+z36+z37+z46+z38+z48$$

$$h01+h02+h03+h21+h22+h14+h24+h33+z31+z32+z41+z43+k4_{38}=v48+z35+z45+z37+z46$$

$$h02+h04+h13+h14+h33+h34+k4_{41}=v11+v31+z21+z31+z33+z42+z34+z43+z36+z45+z37+z47+z48$$

$$h01+h03+h14+h34+k4_{42}=v12+v32+z22+z32+z41+z34+z43+z35+z44+z37+z46+z38+z48$$

$$h01+h02+h11+h04+h31+k4_{43}=v13+v33+z31+z23+z33+z42+z44+z36+z45+z38+z47$$

$$h01+h03+h12+h04+h13+h14+h32+h33+h34+k4_{44}=v14+v34+z32+z41+z24+z33+z42+z35+z36+z46+z47$$

$$h01+h02+h11+h03+h21+h04+h22+h31+h23+h34+k4_{45}=v15+v35+z32+z41+z33+z42+z25+z35+z44+z36+z46+z38+z47$$

$$h02+h03+h12+h21+h04+h22+h31+h23+h32+h24+k4_{46}=v16+z31+v36+z41+z33+z42+z34+z43+z26+z35+z36+z45+z37+z47+z48$$

$$h03+h04+h13+h22+h23+h32+h24+h33+k4_{47}=v17+z32+z41+v37+z42+z34+z43+z35+z44+z27+z36+z37+z46+z38+z48$$

$$h01+h02+h03+h21+h22+h14+h24+h33+z31+k4_{48}=v18+z32+z41+v38+z43+z35+z45+z28+z37+z46$$

$$k5_{11}=v11+v31+v51+z21$$

$$k5_{12}=v12+v32+v52+z22$$

$$k5_{13}=v13+v33+v53+z23$$

$$k5_{14} = v14 + v34 + v54 + z24$$
$$k5_{15} = v15 + v35 + v55 + z25$$
$$k5_{16} = v16 + v36 + v56 + z26$$
$$k5_{17} = v17 + v37 + v57 + z27$$
$$k5_{18} = v18 + v38 + v58 + z28$$
$$h02 + h21 + h13 + h22 + h23 + k5_{21} = v51 + z33 + z34 + z43 + z44 + z37$$
$$h11 + h03 + h21 + h22 + h14 + h23 + h24 + k5_{22} = v52 + z34 + z35 + z44 + z38$$
$$h01 + h11 + h12 + h04 + h22 + h23 + h24 + k5_{23} = v53 + z31 + z41 + z35 + z36$$
$$h01 + h12 + h21 + h22 + h24 + k5_{24} = v54 + z32 + z33 + z42 + z34 + z43 + z44 + z36$$
$$h02 + h03 + h12 + h21 + h04 + h13 + h22 + h14 + h33 + h34 + k5_{25} = v55 + z33 + z36 + z46$$
$$h03 + h04 + h13 + h22 + h14 + h23 + h34 + z31 + k5_{26} = v56 + z34 + z37 + z47$$
$$h21 + h04 + h31 + h14 + h23 + h24 + z31 + z32 + k5_{27} = v57 + z35 + z45 + z38 + z48$$
$$h01 + h02 + h11 + h03 + h12 + h21 + h04 + h13 + h14 + h32 + h24 + h33 + h34 + z32 + z35 + k5_{28} = v58 + z45$$
$$h02 + h12 + h04 + h13 + h23 + h32 + h24 + h34 + k5_{31} = v51 + z43 + z44 + z47$$
$$h01 + h11 + h03 + h13 + h31 + h14 + h24 + h33 + k5_{32} = v52 + z44 + z45 + z48$$
$$h01 + h02 + h12 + h21 + h04 + h31 + h14 + h32 + h34 + k5_{33} = v53 + z41 + z45 + z46$$
$$h01 + h11 + h03 + h12 + h04 + h22 + h31 + h23 + h24 + h33 + h34 + k5_{34} = v54 + z42 + z43 + z44 + z46$$
$$h11 + h21 + h14 + h34 + k5_{35} = v55 + z43 + z46$$
$$h11 + h12 + h22 + h31 + z41 + k5_{36} = v56 + z44 + z47$$
$$h12 + h13 + h23 + h32 + z41 + z42 + k5_{37} = v57 + z45 + z48$$
$$h13 + h24 + h33 + h34 + z42 + k5_{38} = v58 + z45$$
$$h02 + h12 + h04 + h13 + h23 + h32 + h24 + h34 + k5_{41} = v01 + v21 + v41 + z11 + z43 + z44 + z47$$
$$h01 + h11 + h03 + h13 + h31 + h14 + h24 + h33 + k5_{42} = v02 + v22 + v42 + z12 + z44 + z45 + z48$$
$$h01 + h02 + h12 + h21 + h04 + h31 + h14 + h32 + h34 + k5_{43} = v03 + v23 + v43 + z13 + z41 + z45 + z46$$
$$h01 + h11 + h03 + h12 + h04 + h22 + h31 + h23 + h24 + h33 + h34 + k5_{44} = v04 + v24 + v44 + z14 + z42 + z43 + z44 + z46$$
$$h11 + h21 + h14 + h34 + k5_{45} = v05 + v25 + v45 + z15 + z43 + z46$$
$$h11 + h12 + h22 + h31 + k5_{46} = v06 + v26 + z41 + v46 + z16 + z44 + z47$$
$$h12 + h13 + h23 + h32 + k5_{47} = v07 + v27 + z41 + z42 + v47 + z17 + z45 + z48$$
$$h13 + h24 + h33 + h34 + k5_{48} = v08 + v28 + z42 + v48 + z18 + z45$$

$h02+h21+h13+h22+h23+k6_{11}=v11+v31+v51+v61+z21+z33+z34+z43+z44+z37$

$h11+h03+h21+h22+h14+h23+h24+k6_{12}=v12+v32+v52+v62+z22+z34+z35+z44+z38$

$h01+h11+h12+h04+h22+h23+h24+k6_{13}=v13+v33+v53+z31+v63+z23+z41+z35+z36$

$h01+h12+h21+h22+h24+k6_{14}=v14+v34+v54+z32+v64+z24+z33+z42+z34+z43+z44+z36$

$h02+h03+h12+h21+h04+h13+h22+h14+h33+h34+k6_{15}=v15+v35+v55+z33+v65+z25+z36+z46$

$h03+h04+h13+h22+h14+h23+h34+k6_{16}=v16+z31+v36+v56+z34+v66+z26+z37+z47$

$h21+h04+h31+h14+h23+h24+k6_{17}=v17+z31+z32+v37+v57+z35+v67+z27+z45+z38+z48$

$h01+h02+h11+h03+h12+h21+h04+h13+h14+h32+h24+h33+h34+k6_{18}=v18+z32+v38+z35+v58+z45+v68+z28$

$h01+h02+h11+h03+h12+h04+h14+h23+k6_{21}=v61+z32+z33+z42+z43+z35+z36+z38$

$h02+h11+h03+h12+h21+h04+h13+h24+k6_{22}=v62+z31+z41+z33+z34+z43+z35+z44+z36+z37$

$h11+h03+h12+h21+h04+h13+h22+h14+k6_{23}=v63+z32+z42+z34+z35+z44+z36+z37+z38$

$h01+h02+h11+h03+h13+h22+z31+z32+z41+k6_{24}=v64+z42+z35+z37$

$h02+h12+h22+h23+h33+z31+z33+k6_{25}=v65+z34+z36+z37+z46+z47$

$h03+h21+h13+h31+h23+h24+h34+z32+z34+k6_{26}=v66+z35+z45+z37+z38+z47+z48$

$h01+h11+h04+h22+h31+h14+h32+h24+z31+z33+k6_{27}=v67+z36+z46+z38+z48$

$h01+h11+h21+h22+h32+z32+z33+z35+z36+z45+k6_{28}=v68+z46$

$h12+h04+h13+h22+h14+h23+h34+k6_{31}=v61+z42+z43+z45+z46+z48$

$h01+h21+h13+h31+h14+h23+h24+k6_{32}=v62+z41+z43+z44+z45+z46+z47$

$h02+h22+h14+h32+h24+k6_{33}=v63+z42+z44+z45+z46+z47+z48$

$h11+h03+h12+h21+h04+h13+h22+h14+h33+h34+z41+k6_{34}=v64+z42+z45+z47$

$h12+h21+h22+h31+h14+h34+z41+k6_{35}=v65+z43+z44+z46+z47$

$$h11+h13+h22+h31+h23+h32+z42+k6_{36}=v66+z44+z45+z47+z48$$

$$h11+h12+h21+h14+h23+h32+h24+h33+z41+z43+k6_{37}=v67+z46+z48$$

$$h11+h21+h13+h14+h24+h33+z42+z43+z45+k6_{38}=v68+z46$$

$$h12+h04+h13+h22+h14+h23+h34+k6_{41}=v01+v21+v41+z11+z42+z43+z45+z46+z48$$

$$h01+h21+h13+h31+h14+h23+h24+k6_{42}=v02+v22+v42+z12+z41+z43+z44+z45+z46+z47$$

$$h02+h22+h14+h32+h24+k6_{43}=v03+v23+v43+z13+z42+z44+z45+z46+z47+z48$$

$$h11+h03+h12+h21+h04+h13+h22+h14+h33+h34+k6_{44}=v04+v24+v44+z14+z41+z42+z45+z47$$

$$h12+h21+h22+h31+h14+h34+k6_{45}=v05+v25+v45+z41+z15+z43+z44+z46+z47$$

$$h11+h13+h22+h31+h23+h32+k6_{46}=v06+v26+v46+z42+z16+z44+z45+z47+z48$$

$$h11+h12+h21+h14+h23+h32+h24+h33+k6_{47}=v07+v27+z41+v47+z43+z17+z46+z48$$

$$h11+h21+h13+h14+h24+h33+k6_{48}=v08+v28+z42+z43+v48+z18+z45+z46$$

$$h01+h11+h03+h12+h13+h23+h33+h34+k7_{11}=v01+v21+v41+z11+v71+z31+z32+z34+z35+z45+z37+z38+z47+z48$$

$$h01+h02+h11+h12+h21+h04+h13+h14+h24+h34+k7_{12}=v02+v22+v42+z12+z31+v72+z32+z33+z36+z46+z38+z48$$

$$h01+h02+h03+h12+h21+h13+h22+h31+h14+k7_{13}=v03+v23+v43+z13+z31+z32+v73+z33+z34+z35+z45+z37+z47$$

$$h02+h11+h12+h04+h22+h14+h32+h33+h34+k7_{14}=v04+v24+v44+z31+z14+z33+v74+z36+z37+z46+z47$$

$$h01+h11+h03+h12+h21+h04+h31+h33+h34+k7_{15}=v05+v25+z31+v45+z32+z41+z15+z42+z34+v75+z35+z44+z37+z38$$

$$h02+h12+h04+h13+h22+h32+h34+k7_{16}=v06+v26+z31+z32+z41+v46+z33+z42+z16+z43+v76+z36+z38$$

$$h01+h11+h03+h13+h31+h14+h23+h33+k7_{17}=v07+z31+v27+z32+z41+z33+z42+v47+z34+z43+z17+z35+z44+v77+z37$$

$$h02+h11+h03+h14+h32+h24+h33+k7_{18}=v08+z31+z41+v28+z33+z43+v48+z18+z36+z37+v78$$

$$h01+h21+h13+h32+h33+k7_{21}=v71+z32+z37+z38+z47+z48$$

$$h02+h11+h22+h31+h14+h33+h34+k7_{22}=v72+z33+z38+z48$$

$$h11+h03+h12+h23+h32+h34+z31+k7_{23}=v73+z34+z35+z45$$

$$h12+h04+h31+h32+h24+z31+k7_{24}=v74+z36+z37+z46+z38+z47+z48$$

$$h01+h02+h03+h12+h21+h13+h22+h31+h32+h33+z33+z34+z43+k7_{25}=v75+z35+z44+z36+z37$$

$$h01+h02+h11+h03+h04+h13+h22+h31+h14+h23+h32+h33+h34+z34+z35+z44+k7_{26}=v76+z36+z37+z38$$

$$h02+h03+h12+h21+h04+h14+h23+h32+h24+h33+h34+z31+z41+z36+k7_{27}=v77+z37+z38$$

$$h01+h02+h11+h12+h21+h04+h31+h32+h24+h34+z32+z33+z42+z34+z43+z35+z44+z36+k7_{28}=v78+z38$$

$$h12+h04+h13+h32+h33+k7_{31}=v71+z33+z42+z34+z43+z44+z36+z37+z38+z47+z48$$

$$h01+h11+h13+h31+h14+h33+h34+k7_{32}=v72+z34+z43+z44+z37+z38+z48$$

$$h02+h12+h14+h32+h34+z31+k7_{33}=v73+z44+z45+z38$$

$$h11+h03+h12+h04+h31+h32+z32+z41+z33+z42+k7_{34}=v74+z34+z43+z35+z44+z36+z37+z46+z38+z47+z48$$

$$h01+h11+h12+h32+h24+h34+z31+z32+z34+z43+k7_{35}=v75+z44+z45+z37+z46+z38+z48$$

$$h02+h12+h21+h13+h31+h33+z31+z32+z33+z44+k7_{36}=v76+z45+z46+z38+z47$$

$$h11+h03+h13+h22+h31+h14+h32+h34+z31+z32+z41+z33+z34+z35+z45+k7_{37}=v77+z46+z47+z48$$

$$h11+h04+h31+h14+h23+h24+h33+h34+z31+z33+z42+z43+z44+z36+z45+z37+k7_{38}=v78+z38+z47$$

$$h12+h04+h13+h32+h33+k7_{41}=v11+v31+v51+v61+z21+z33+z42+z34+z43+z44+z36+z37+z38+z47+z48$$

$$h01+h11+h13+h31+h14+h33+h34+k7_{42}=v12+v32+v52+v62+z22+z34+z43+z44+z37+z38+z48$$

$$h02+h12+h14+h32+h34+k7_{43}=v13+v33+v53+z31+v63+z23+z44+z45+z38$$

$$h11+h03+h12+h04+h31+h32+k7_{44}=v14+v34+v54+z32+z41+v64+z24+z33+z42+z34+z43+z35+z44+z36+z37+z46+z38+z47+z48$$

$$h01+h11+h12+h32+h24+h34+k7_{45}=v15+v35+z31+z32+v55+v65+z25+z34+z43+z44+z45+z37+z46+z38+z48$$

$$h02+h12+h21+h13+h31+h33+k7_{46}=v16+z31+v36+z32+z33+v56+v66+z26+z44+z45+z46+z38+z47$$

$$h11+h03+h13+h22+h31+h14+h32+h34+k7_{47}=v17+z31+z32+z41+v37+z33+z34+v57+z35+v67+z27+z45+z46+z47+z48$$

$h11 + h04 + h31 + h14 + h23 + h24 + h33 + h34 + z31 + k7_{48} = v18 + z33 + z42 + v38 + z43 + z44 + v58 + z36 + z45 + v68 + z28 + z37 + z38 + z47$

$h02 + h03 + h04 + h13 + h22 + h31 + h32 + h33 + k8_{11} = v11 + v31 + v51 + v61 + z21 + v81 + z32 + z42 + z35 + z37$

$h11 + h03 + h04 + h31 + h14 + h23 + h32 + h33 + h34 + k8_{12} = v12 + v32 + v52 + v62 + z22 + v82 + z33 + z43 + z35 + z36 + z38$

$h11 + h12 + h21 + h04 + h32 + h24 + h33 + h34 + k8_{13} = v13 + v33 + v53 + z31 + v63 + z23 + z41 + v83 + z34 + z35 + z44 + z36 + z37$

$h01 + h02 + h03 + h12 + h21 + h04 + h31 + h32 + h34 + k8_{14} = v14 + v34 + z31 + v54 + z41 + v64 + z24 + v84 + z36 + z38$

$h01 + h02 + h11 + h03 + h22 + h31 + h32 + h24 + h34 + k8_{15} = v15 + v35 + z31 + v55 + z33 + v65 + z25 + z35 + v85 + z36 + z45 + z37 + z46 + z47$

$h01 + h02 + h03 + h12 + h21 + h04 + h31 + h23 + h32 + h33 + k8_{16} = v16 + z31 + v36 + z32 + v56 + z34 + v66 + z26 + z35 + z36 + z45 + v86 + z37 + z46 + z38 + z47 + z48$

$h02+h03+h21+h04+h13+h22+h31+h32+h24+h33+h34+k8_{17} = v17+z31+z32+v37+z33+v57+v67+z27+z36+z37+z46+v87+z38+z47+z48$

$h01 + h02 + h21 + h04 + h31 + h14 + h23 + h24 + h33 + k8_{18} = v18 + z32 + v38 + z34 + z35 + v58 + z36 + z45 + v68 + z28 + z46 + z38 + v88 + z48$

$h01+h02+h11+h21+h23+h33+z31+k8_{21} = v81+z41+z33+z43+z35$

$h02+h03+h12+h21+h22+h31+h24+h34+z31+z32+z41+k8_{22} = v82 + z42 + z34 + z44 + z36$

$h01 + h03 + h21 + h04 + h13 + h22 + h31 + h23 + h32 + z31 + z32 + z41 + z33 + z42 + k8_{23} = v83 + z43 + z37$

$h01+h04+h22+h14+h32+h24+z32+z42+z34+k8_{24} = v84+z44+z38$

$h11+h12+h21+h04+h22+h31+h23+h32+h24+h33+h34+z32+z33+z34+k8_{25} = v85 + z38 + z48$

$h01 + h12 + h13 + h22 + h23 + h32 + h24 + h33 + h34 + z33 + z34 + z35 + z45 + k8_{26} = v86$

$h02+h11+h13+h14+h23+h24+h33+h34+z34+z36+z46+k8_{27} = v87$

$h11 + h03 + h21 + h04 + h22 + h31 + h14 + h23 + h32 + h33 + z31 + z32 + z33 + z34 + z37 + z38 + z47 + k8_{28} = v88 + z48$

$h01 + h21 + h04 + h22 + h23 + h32 + h24 + h34 + k8_{31} = v81 + z41 + z43 + z35 + z36 + z37 + z46 + z47$

$h01 + h02 + h22 + h31 + h23 + h24 + h33 + z41 + k8_{32} = v82 + z42 + z35 + z44 + z36 + z45 + z37 + z38 + z47 + z48$

$h02 + h03 + h31 + h23 + h32 + h24 + h34 + z41 + z42 + k8_{33} = v83 + z43 + z36 + z37 + z46 + z38 + z48$

$h03 + h21 + h22 + h31 + h23 + h33 + h34 + z42 + k8_{34} = v84 + z35 +$

$$z44 + z36 + z45 + z46 + z38$$

$$h22 + h14 + h24 + h33 + z32 + z34 + z43 + k8_{35} = v85 + z48$$

$$h11 + h21 + h31 + h23 + h34 + z31 + z41 + z33 + z44 + z45 + k8_{36} = v86$$

$$h12+h21+h22+h31+h32+h24+z31+z32+z41+z42+z34+z46+k8_{37} = v87$$

$$h21 + h13 + h14 + h23 + h32 + h24 + z31 + z33 + z42 + z34 + z47 + k8_{38} = v88 + z48$$

$$h01 + h21 + h04 + h22 + h23 + h32 + h24 + h34 + k8_{41} = v01 + v21 + v41 + z11 + v71 + z41 + z43 + z35 + z36 + z37 + z46 + z47$$

$$h01 + h02 + h22 + h31 + h23 + h24 + h33 + k8_{42} = v02 + v22 + v42 + z12 + v72 + z41 + z42 + z35 + z44 + z36 + z45 + z37 + z38 + z47 + z48$$

$$h02 + h03 + h31 + h23 + h32 + h24 + h34 + k8_{43} = v03 + v23 + v43 + z13 + z41 + v73 + z42 + z43 + z36 + z37 + z46 + z38 + z48$$

$$h03 + h21 + h22 + h31 + h23 + h33 + h34 + k8_{44} = v04 + v24 + v44 + z14 + z42 + v74 + z35 + z44 + z36 + z45 + z46 + z38$$

$$h22 + h14 + h24 + h33 + k8_{45} = v05 + v25 + v45 + z32 + z15 + z34 + z43 + v75 + z48$$

$$h11 + h21 + h31 + h23 + h34 + k8_{46} = v06 + v26 + z31 + z41 + v46 + z33 + z16 + z44 + v76 + z45$$

$$h12 + h21 + h22 + h31 + h32 + h24 + k8_{47} = v07 + z31 + v27 + z32 + z41 + z42 + v47 + z34 + z17 + v77 + z46$$

$$h21 + h13 + h14 + h23 + h32 + h24 + k8_{48} = v08 + z31 + v28 + z33 + z42 + z34 + v48 + z18 + v78 + z47 + z48$$

$$h02 + h12 + h21 + h31 + h23 + k9_{11} = v01 + v21 + v41 + z11 + v71 + z31 + z32 + v91 + z34 + z36 + z37 + z46 + z38 + z47 + z48$$

$$h03 + h21 + h13 + h22 + h32 + h24 + k9_{12} = v02 + v22 + v42 + z12 + z31 + v72 + z32 + z33 + v92 + z37 + z38 + z47 + z48$$

$$h01 + h11 + h21 + h04 + h22 + h14 + h23 + h33 + k9_{13} = v03 + v23 + v43 + z13 + z31 + z32 + v73 + z33 + z34 + v93 + z38 + z48$$

$$h01 + h11 + h22 + h24 + h34 + k9_{14} = v04 + v24 + v44 + z31 + z14 + z33 + v74 + z35 + v94 + z36 + z45 + z37 + z46 + z38 + z47 + z48$$

$$h01 + h02 + h12 + h04 + h31 + h14 + h32 + h33 + h34 + k9_{15} = v05 + v25 + z31 + v45 + z41 + z15 + v75 + z35 + v95 + z38$$

$$h01 + h02 + h11 + h03 + h13 + h32 + h33 + h34 + k9_{16} = v06 + v26 + z32 + v46 + z42 + z16 + z35 + v76 + z36 + v96$$

$$h01 + h02 + h11 + h03 + h12 + h04 + h14 + h33 + h34 + k9_{17} = v07 + v27 + z33 + v47 + z43 + z17 + z36 + v77 + z37 + v97$$

$$h01 + h11 + h03 + h13 + h31 + h14 + h32 + h33 + k9_{18} = v08 + v28 + z34 + v48 + z44 + z18 + z37 + v78 + v98$$

$$h01+h11+h03+h21+h13+z32+k9_{21}=v91+z35+z36+z45+z46$$
$$h01+h02+h11+h12+h04+h22+h14+z33+k9_{22}=v92+z36+z37+z46+z47$$
$$h01+h02+h11+h03+h12+h13+h23+z31+z34+k9_{23}=v93+z35+z45+z37+z38+z47+z48$$
$$h02+h12+h04+h14+h24+z31+z35+k9_{24}=v94+z45+z38+z48$$
$$h01+h02+h11+h03+h12+h04+h13+h31+h14+z31+z32+z41+z42+z36+k9_{25}=v95+z38$$
$$h02+h03+h12+h04+h13+h14+h32+z32+z33+z42+z43+z35+z37+k9_{26}=v96$$
$$h03+h04+h13+h14+h33+z31+z41+z33+z34+z43+z35+z44+z36+z38+k9_{27}=v97$$
$$h01+h02+h11+h03+h12+h13+h34+z31+z41+z34+z35+z44+z37+z38+k9_{28}=v98$$

【０１１０】

次に、ステップＳ１０４の行列方程式変換処理を実行する。ここで、ベクトルＫ，Ｈ，Ｕ，Ｖを下記のように設定する。

【０１１１】

【数３５】

Ｋ＝（ｋ１$_{11}$，Ｋ１$_{12}$，．．．，ｋ９$_{28}$）

Ｈ＝（ｈ０１，ｈ０２，．．．，ｈ４４）

Ｕ＝（ｚ１１，ｚ１２，．．．，ｚ４４）

Ｖ＝（ｖ０１，ｖ０２，．．．ｖ７４）

【０１１２】

上記式のように、ベクトルＫ，Ｈ，Ｕ，Ｖを設定すると、上記連立線形方程式は以下のように行列方程式に変換できる。

【０１１３】

【数３６】

$$M_{KH}\begin{pmatrix}{}^tK\\{}^tH\end{pmatrix}=M_{UV}\begin{pmatrix}{}^tU\\{}^tV\end{pmatrix}$$

【０１１４】

なお、上記式において、M_{KH}，M_{UV}は、上記連立線形方程式の係数から成るＧＦ（２）上の行列である。

【０１１５】

次に、ステップＳ１０５のユニタリ変換処理を実行する。

【０１１６】

【数３７】

$$rank(M_{UV}) = N_r$$

【０１１７】

とする。また、行列M_{UV}の行数をN_mとする。上記行列方程式の両辺に左から行変形ユニタリー行列Ｑを乗ずることによって、行列M_{UV}を階段行列に変形することができる。このとき、QM_{UV}のうち、下$N_m - N_r$行から成る小行列は零行列になる。

【０１１８】

次に、ステップＳ１０６の小行列選択処理を実行する。QM_{KH}の下$N_m - N_r$行の小行列をM^*_{KH}とおくと、M^*_{KH}は零行列（Ｏ）であり、下記式によって示される。

【０１１９】

【数３８】

$$M^*_{KH} = O$$

【０１２０】

次にステップＳ１０７の線形関係式生成処理を実行する。この行列方程式を行毎の線形関係式に変換し、h01,h02,．．．,h44の具体的値を代入すると、以下のような関係式が得られる。

【０１２１】

【数３９】

$$0x07 = k1_{11} + k1_{21} + k1_{24} + k1_{26} + k1_{31} + k1_{34} + k1_{36} + k1_{42} + k2_{12} + k2_{22} + k3_{11} + k3_{21}$$

$$0x66 = k1_{12} + k1_{21} + k1_{22} + k1_{27} + k1_{31} + k1_{32} + k1_{37} + k1_{43} + k2_{13} + k2_{23} + k3_{12} + k3_{22}$$

$$0x9e = k1_{13} + k1_{22} + k1_{23} + k1_{25} + k1_{28} + k1_{32} + k1_{33} + k1_{35} + k1_{38} + k1_{41} + k1_{44} + k2_{11} + k2_{14} + k2_{21} + k2_{24} + k3_{13} + k3_{23}$$

$$0xdf = k1_{14} + k1_{23} + k1_{25} + k1_{33} + k1_{35} + k1_{41} + k2_{11} + k2_{21} + k3_{14} + k3_{24}$$

$$0xe9 = k1_{15} + k1_{22} + k1_{24} + k1_{25} + k1_{26} + k1_{32} + k1_{34} + k1_{35} + k1_{36} + k1_{46} + k1_{48} + k2_{16} + k2_{18} + k2_{26} + k2_{28} + k3_{15} + k3_{25}$$

$$0x23 = k1_{16} + k1_{21} + k1_{23} + k1_{26} + k1_{27} + k1_{31} + k1_{33} + k1_{36} + k1_{37} + k1_{45} + k1_{47} + k2_{15} + k2_{17} + k2_{25} + k2_{27} + k3_{16} + k3_{26}$$

$$0x60 = k1_{17} + k1_{21} + k1_{22} + k1_{24} + k1_{25} + k1_{27} + k1_{28} + k1_{31} + k1_{32} + k1_{34} + k1_{35} + k1_{37} + k1_{38} + k1_{45} + k1_{46} + k1_{48} + k2_{15} + k2_{16} + k2_{18} + k2_{25} + k2_{26} + k2_{28} + k3_{17} + k3_{27}$$

$$0xcd = k1_{18} + k1_{21} + k1_{23} + k1_{24} + k1_{25} + k1_{28} + k1_{31} + k1_{33} + k1_{34} + k1_{35} + k1_{38} + k1_{45} + k1_{47} + k1_{48} + k2_{15} + k2_{17} + k2_{18} + k2_{25} + k2_{27} + k2_{28} + k3_{18} + k3_{28}$$

$$0x3d = k1_{21} + k1_{24} + k1_{27} + k1_{28} + k1_{31} + k1_{34} + k1_{37} + k1_{38} + k1_{41} + k1_{42} + k1_{43} + k1_{48} + k2_{11} + k2_{12} + k2_{18} + k2_{21} + k2_{22} + k2_{23} + k2_{28} + k4_{13} + k4_{33}$$

$$0x90 = k1_{22} + k1_{25} + k1_{26} + k1_{27} + k1_{28} + k1_{32} + k1_{35} + k1_{36} + k1_{37} + k1_{38} + k1_{41} + k1_{43} + k1_{46} + k1_{47} + k1_{48} + k2_{13} + k2_{16} + k2_{17} + k2_{18} + k2_{21} + k2_{23} + k2_{26} + k2_{27} + k2_{28} + k4_{11} + k4_{31}$$

$$0xc1 = k1_{23} + k1_{26} + k1_{27} + k1_{28} + k1_{33} + k1_{36} + k1_{37} + k1_{38} + k1_{41} + k1_{42} + k1_{44} + k1_{47} + k1_{48} + k2_{11} + k2_{14} + k2_{17} + k2_{18} + k2_{21} + k2_{22} + k2_{24} + k2_{27} + k2_{28} + k4_{12} + k4_{32}$$

$$0x80 = k1_{24} + k1_{25} + k1_{26} + k1_{28} + k1_{34} + k1_{35} + k1_{36} + k1_{38} + k1_{41} + k1_{43} + k1_{44} + k1_{45} + k1_{46} + k1_{47} + k2_{11} + k2_{15} + k2_{16} + k2_{17} + k2_{21} + k2_{23} + k2_{24} + k2_{25} + k2_{26} + k2_{27} + k4_{13} + k4_{14} + k4_{33} + k4_{34}$$

$$0x39 = k1_{25} + k1_{35} + k1_{41} + k1_{44} + k1_{45} + k1_{47} + k1_{48} + k2_{11} + k2_{12} + k2_{14} + k2_{15} + k2_{16} + k2_{17} + k2_{18} + k2_{21} + k2_{24} + k2_{25} + k2_{27} + k2_{28} + k4_{12} + k4_{16} + k4_{32} + k4_{36}$$

$$0x2d = k1_{26} + k1_{36} + k1_{41} + k1_{42} + k1_{46} + k1_{48} + k2_{11} + k2_{12} + k2_{13} + k2_{16} + k2_{17} + k2_{18} + k2_{21} + k2_{22} + k2_{26} + k2_{28} + k4_{13} + k4_{17} + k4_{33} + k4_{37}$$

$$0xd5 = k1_{27} + k1_{28} + k1_{37} + k1_{38} + k1_{42} + k1_{45} + k1_{46} + k2_{12} + k2_{14} + k2_{15} + k2_{16} + k2_{18} + k2_{22} + k2_{25} + k2_{26} + k4_{14} + k4_{18} + k4_{34} + k4_{38}$$

$$0xfa = k1_{28} + k1_{38} + k1_{43} + k1_{46} + k1_{47} + k2_{11} + k2_{13} + k2_{15} + k2_{16} + k2_{17} + k2_{23} + k2_{26} + k2_{27} + k4_{11} + k4_{15} + k4_{31} + k4_{35}$$

$$0x39 = k1_{41} + k1_{42} + k1_{44} + k1_{46} + k1_{48} + k2_{12} + k2_{13} + k2_{17} + k2_{18} + k2_{22} + k2_{24} + k2_{26} + k2_{28} + k2_{31} + k4_{11} + k4_{13} + k4_{14} + k4_{16} + k4_{17} + k4_{31} + k4_{33} + k4_{34} + k4_{36} + k4_{37}$$

$$0x35 = k1_{42} + k1_{43} + k1_{44} + k1_{45} + k1_{46} + k1_{47} + k2_{11} + k2_{13} + k2_{16} + k2_{21} + k2_{22} + k2_{23} + k2_{25} + k2_{26} + k2_{27} + k2_{31} + k2_{34} + k4_{11} + k4_{12} + k4_{14} +$$

$k4_{15} + k4_{17} + k4_{31} + k4_{32} + k4_{34} + k4_{35} + k4_{37}$

$0x4b = k1_{43} + k1_{44} + k1_{45} + k1_{46} + k1_{47} + k1_{48} + k2_{11} + k2_{12} + k2_{14} + k2_{17} + k2_{21} + k2_{22} + k2_{23} + k2_{24} + k2_{25} + k2_{26} + k2_{27} + k2_{28} + k2_{31} + k2_{32} + k4_{11} + k4_{12} + k4_{13} + k4_{15} + k4_{16} + k4_{18} + k4_{31} + k4_{32} + k4_{33} + k4_{35} + k4_{36} + k4_{38}$

$0xe7 = k1_{44} + k1_{46} + k1_{47} + k1_{48} + k2_{11} + k2_{12} + k2_{13} + k2_{15} + k2_{18} + k2_{22} + k2_{23} + k2_{24} + k2_{26} + k2_{27} + k2_{28} + k2_{32} + k2_{33} + k4_{11} + k4_{12} + k4_{13} + k4_{14} + k4_{15} + k4_{16} + k4_{17} + k4_{31} + k4_{32} + k4_{33} + k4_{34} + k4_{35} + k4_{36} + k4_{37}$

$0x33 = k1_{45} + k1_{46} + k2_{12} + k2_{13} + k2_{14} + k2_{16} + k2_{21} + k2_{25} + k2_{26} + k2_{31} + k3_{11} + k4_{12} + k4_{13} + k4_{14} + k4_{15} + k4_{32} + k4_{33} + k4_{34} + k4_{35} + k5_{11} + k5_{21}$

$0xdb = k1_{46} + k1_{47} + k2_{13} + k2_{14} + k2_{17} + k2_{22} + k2_{26} + k2_{27} + k2_{32} + k3_{12} + k4_{13} + k4_{14} + k4_{16} + k4_{33} + k4_{34} + k4_{36} + k5_{12} + k5_{22}$

$0x8f = k1_{47} + k1_{48} + k2_{11} + k2_{13} + k2_{14} + k2_{15} + k2_{16} + k2_{17} + k2_{21} + k2_{22} + k2_{24} + k2_{27} + k2_{28} + k2_{31} + k2_{32} + k2_{34} + k3_{11} + k3_{12} + k3_{14} + k4_{11} + k4_{13} + k4_{14} + k4_{15} + k4_{16} + k4_{18} + k4_{31} + k4_{33} + k4_{34} + k4_{35} + k4_{36} + k4_{38} + k5_{11} + k5_{12} + k5_{14} + k5_{21} + k5_{22} + k5_{24}$

$0x83 = k1_{48} + k2_{12} + k2_{14} + k2_{15} + k2_{16} + k2_{17} + k2_{18} + k2_{21} + k2_{22} + k2_{23} + k2_{28} + k2_{31} + k2_{32} + k2_{33} + k3_{11} + k3_{12} + k3_{13} + k4_{12} + k4_{14} + k4_{15} + k4_{16} + k4_{17} + k4_{32} + k4_{34} + k4_{35} + k4_{36} + k4_{37} + k5_{11} + k5_{12} + k5_{13} + k5_{21} + k5_{22} + k5_{23}$

$0x00 = k2_{11} + k3_{11} + k4_{11} + k4_{31} + k4_{41}$

$0x00 = k2_{12} + k3_{12} + k4_{12} + k4_{32} + k4_{42}$

$0x00 = k2_{13} + k3_{13} + k4_{13} + k4_{33} + k4_{43}$

$0x00 = k2_{14} + k3_{14} + k4_{14} + k4_{34} + k4_{44}$

$0x1f = k2_{15} + k2_{17} + k2_{22} + k2_{23} + k2_{24} + k2_{25} + k2_{32} + k2_{33} + k2_{34} + k2_{35} + k3_{11} + k3_{12} + k3_{13} + k3_{14} + k4_{15} + k4_{17} + k4_{35} + k4_{37} + k4_{41} + k4_{42} + k4_{43} + k4_{44}$

$0x8e = k2_{16} + k2_{17} + k2_{18} + k2_{22} + k2_{25} + k2_{26} + k2_{32} + k2_{35} + k2_{36} + k3_{11} + k4_{16} + k4_{17} + k4_{18} + k4_{36} + k4_{37} + k4_{38} + k4_{41}$

$0x68 = k2_{17} + k2_{18} + k2_{23} + k2_{26} + k2_{27} + k2_{33} + k2_{36} + k2_{37} + k3_{12} + k4_{17} + k4_{18} + k4_{37} + k4_{38} + k4_{42}$

$0x35 = k2_{18} + k2_{21} + k2_{24} + k2_{25} + k2_{27} + k2_{28} + k2_{31} + k2_{34} + k2_{35} + k2_{37} + k2_{38} + k3_{13} + k4_{18} + k4_{38} + k4_{43}$

$0x42 = k2_{21} + k2_{22} + k2_{26} + k2_{28} + k2_{31} + k2_{32} + k2_{36} + k2_{38} + k3_{11} + k3_{14} + k3_{15} + k4_{41} + k4_{44} + k4_{45}$

$0xe6 = k2_{22} + k2_{23} + k2_{25} + k2_{27} + k2_{32} + k2_{33} + k2_{35} + k2_{37} + k3_{11} + k3_{12} + k3_{16} + k4_{41} + k4_{42} + k4_{46}$

$0x91 = k2_{23} + k2_{24} + k2_{26} + k2_{33} + k2_{34} + k2_{36} + k3_{12} + k3_{13} + k3_{14} + k3_{15} + k3_{16} + k3_{18} + k4_{42} + k4_{43} + k4_{44} + k4_{45} + k4_{46} + k4_{48}$

$0xf9 = k2_{24} + k2_{27} + k2_{34} + k2_{37} + k3_{13} + k3_{14} + k3_{15} + k3_{16} + k3_{17} + k4_{43} + k4_{44} + k4_{45} + k4_{46} + k4_{47}$

$0xa0 = k2_{25} + k2_{28} + k2_{35} + k2_{38} + k3_{11} + k3_{13} + k3_{15} + k4_{44} + k5_{11} +$

$k5_{13} + k5_{14} + k5_{15} + k5_{21} + k5_{23} + k5_{24} + k5_{25}$

$0xb7 = k2_{26} + k2_{28} + k2_{36} + k2_{38} + k3_{12} + k3_{13} + k3_{14} + k3_{15} + k3_{16} + k4_{41} + k4_{44} + k5_{11} + k5_{12} + k5_{13} + k5_{15} + k5_{16} + k5_{21} + k5_{22} + k5_{23} + k5_{25} + k5_{26}$

$0x07 = k2_{27} + k2_{28} + k2_{37} + k2_{38} + k3_{11} + k3_{14} + k3_{15} + k3_{16} + k3_{17} + k4_{41} + k4_{42} + k4_{44} + k5_{12} + k5_{15} + k5_{16} + k5_{17} + k5_{22} + k5_{25} + k5_{26} + k5_{27}$

$0xc1 = k2_{28} + k2_{38} + k3_{11} + k3_{12} + k3_{15} + k3_{16} + k3_{17} + k3_{18} + k4_{41} + k4_{42} + k4_{43} + k5_{13} + k5_{15} + k5_{16} + k5_{17} + k5_{18} + k5_{23} + k5_{25} + k5_{26} + k5_{27} + k5_{28}$

$0xc9 = k2_{41} + k3_{11} + k3_{12} + k3_{13} + k3_{16} + k3_{17} + k3_{21} + k4_{41} + k4_{42} + k4_{43} + k4_{47} + k4_{48} + k5_{11} + k5_{16} + k5_{18} + k5_{21} + k5_{26} + k5_{28}$

$0xed = k2_{42} + k3_{11} + k3_{12} + k3_{13} + k3_{14} + k3_{15} + k3_{17} + k3_{18} + k3_{22} + k4_{41} + k4_{42} + k4_{43} + k4_{44} + k4_{48} + k5_{12} + k5_{15} + k5_{17} + k5_{22} + k5_{25} + k5_{27}$

$0xf6 = k2_{43} + k3_{12} + k3_{13} + k3_{14} + k3_{16} + k3_{18} + k3_{23} + k4_{42} + k4_{43} + k4_{44} + k4_{45} + k5_{13} + k5_{15} + k5_{16} + k5_{18} + k5_{23} + k5_{25} + k5_{26} + k5_{28}$

$0x46 = k2_{44} + k3_{11} + k3_{12} + k3_{14} + k3_{15} + k3_{16} + k3_{24} + k4_{41} + k4_{42} + k4_{44} + k4_{46} + k4_{47} + k4_{48} + k5_{14} + k5_{15} + k5_{17} + k5_{18} + k5_{24} + k5_{25} + k5_{27} + k5_{28}$

$0x81 = k2_{45} + k3_{11} + k3_{14} + k3_{15} + k3_{16} + k3_{17} + k3_{18} + k3_{25} + k4_{41} + k4_{43} + k4_{46} + k4_{48} + k5_{13} + k5_{14} + k5_{17} + k5_{23} + k5_{24} + k5_{27}$

$0x29 = k2_{46} + k3_{11} + k3_{12} + k3_{16} + k3_{17} + k3_{18} + k3_{26} + k4_{41} + k4_{42} + k4_{44} + k4_{45} + k4_{47} + k5_{14} + k5_{15} + k5_{18} + k5_{24} + k5_{25} + k5_{28}$

$0x85 = k2_{47} + k3_{12} + k3_{13} + k3_{17} + k3_{18} + k3_{27} + k4_{41} + k4_{42} + k4_{43} + k4_{45} + k4_{46} + k4_{48} + k5_{11} + k5_{15} + k5_{16} + k5_{21} + k5_{25} + k5_{26}$

$0x69 = k2_{48} + k3_{13} + k3_{15} + k3_{16} + k3_{17} + k3_{28} + k4_{42} + k4_{44} + k4_{45} + k4_{47} + k4_{48} + k5_{12} + k5_{13} + k5_{14} + k5_{16} + k5_{22} + k5_{23} + k5_{24} + k5_{26}$

$0x7b = k3_{11} + k3_{13} + k3_{16} + k3_{17} + k3_{18} + k4_{11} + k4_{41} + k4_{43} + k5_{16} + k5_{17} + k5_{18} + k5_{26} + k5_{27} + k5_{28} + k5_{41}$

$0x1b = k3_{12} + k3_{13} + k3_{14} + k3_{16} + k4_{11} + k4_{12} + k4_{42} + k4_{43} + k4_{44} + k5_{16} + k5_{26} + k5_{41} + k5_{42}$

$0xbc = k3_{13} + k3_{14} + k3_{17} + k4_{12} + k4_{13} + k4_{43} + k4_{44} + k5_{17} + k5_{27} + k5_{42} + k5_{43}$

$0x53 = k3_{14} + k3_{15} + k3_{18} + k4_{11} + k4_{13} + k4_{14} + k4_{44} + k5_{15} + k5_{18} + k5_{25} + k5_{28} + k5_{41} + k5_{43} + k5_{44}$

$0x04 = k3_{15} + k3_{17} + k4_{11} + k4_{12} + k4_{13} + k4_{15} + k4_{41} + k4_{44} + k4_{45} + k4_{46} + k4_{47} + k4_{48} + k5_{11} + k5_{14} + k5_{16} + k5_{18} + k5_{21} + k5_{24} + k5_{26} + k5_{28} + k5_{41} + k5_{42} + k5_{43} + k5_{45}$

$0xef = k3_{16} + k3_{17} + k3_{18} + k4_{14} + k4_{15} + k4_{16} + k4_{42} + k4_{44} + k4_{45} + k5_{12} + k5_{14} + k5_{15} + k5_{16} + k5_{17} + k5_{18} + k5_{22} + k5_{24} + k5_{25} + k5_{26} + k5_{27} + k5_{28} + k5_{44} + k5_{45} + k5_{46}$

$0x58 = k3_{17} + k3_{18} + k4_{11} + k4_{16} + k4_{17} + k4_{41} + k4_{43} + k4_{46} + k5_{11} + k5_{13} + k5_{16} + k5_{17} + k5_{18} + k5_{21} + k5_{23} + k5_{26} + k5_{27} + k5_{28} + k5_{41} + k5_{46} + k5_{47}$

$$0x21 = k3_{18} + k4_{12} + k4_{15} + k4_{17} + k4_{18} + k4_{41} + k4_{42} + k4_{44} + k4_{47} + k5_{11} + k5_{12} + k5_{14} + k5_{17} + k5_{18} + k5_{21} + k5_{22} + k5_{24} + k5_{27} + k5_{28} + k5_{42} + k5_{45} + k5_{47} + k5_{48}$$

$$0x37 = k3_{21} + k3_{31} + k4_{11} + k4_{12} + k4_{13} + k4_{14} + k4_{16} + k4_{17} + k4_{18} + k4_{41} + k4_{44} + k4_{45} + k4_{47} + k5_{11} + k5_{14} + k5_{15} + k5_{17} + k5_{21} + k5_{24} + k5_{25} + k5_{27} + k5_{41} + k5_{42} + k5_{43} + k5_{44} + k5_{46} + k5_{47} + k5_{48}$$

$$0xa3 = k3_{22} + k3_{32} + k4_{12} + k4_{13} + k4_{14} + k4_{17} + k4_{18} + k4_{41} + k4_{42} + k4_{45} + k4_{46} + k4_{48} + k5_{11} + k5_{12} + k5_{15} + k5_{16} + k5_{18} + k5_{21} + k5_{22} + k5_{25} + k5_{26} + k5_{28} + k5_{42} + k5_{43} + k5_{44} + k5_{47} + k5_{48}$$

$$0x9b = k3_{23} + k3_{33} + k4_{13} + k4_{14} + k4_{18} + k4_{42} + k4_{43} + k4_{45} + k4_{46} + k4_{47} + k5_{12} + k5_{13} + k5_{15} + k5_{16} + k5_{17} + k5_{22} + k5_{23} + k5_{25} + k5_{26} + k5_{27} + k5_{43} + k5_{44} + k5_{48}$$

$$0x51 = k3_{24} + k3_{34} + k4_{11} + k4_{12} + k4_{13} + k4_{15} + k4_{16} + k4_{17} + k4_{18} + k4_{43} + k4_{46} + k4_{48} + k5_{13} + k5_{16} + k5_{18} + k5_{23} + k5_{26} + k5_{28} + k5_{41} + k5_{42} + k5_{43} + k5_{45} + k5_{46} + k5_{47} + k5_{48}$$

$$0x4a = k3_{25} + k3_{35} + k4_{12} + k4_{14} + k4_{16} + k4_{17} + k4_{18} + k4_{41} + k4_{46} + k4_{47} + k5_{11} + k5_{16} + k5_{17} + k5_{21} + k5_{26} + k5_{27} + k5_{42} + k5_{44} + k5_{46} + k5_{47} + k5_{48}$$

$$0x5f = k3_{26} + k3_{36} + k4_{11} + k4_{13} + k4_{17} + k4_{18} + k4_{42} + k4_{45} + k4_{47} + k4_{48} + k5_{12} + k5_{15} + k5_{17} + k5_{18} + k5_{22} + k5_{25} + k5_{27} + k5_{28} + k5_{41} + k5_{43} + k5_{47} + k5_{48}$$

$$0x9a = k3_{27} + k3_{37} + k4_{11} + k4_{12} + k4_{14} + k4_{18} + k4_{43} + k4_{46} + k4_{48} + k5_{13} + k5_{16} + k5_{18} + k5_{23} + k5_{26} + k5_{28} + k5_{41} + k5_{42} + k5_{44} + k5_{48}$$

$$0xc2 = k3_{28} + k3_{38} + k4_{11} + k4_{13} + k4_{14} + k4_{15} + k4_{16} + k4_{17} + k4_{18} + k4_{44} + k4_{45} + k4_{46} + k5_{14} + k5_{15} + k5_{16} + k5_{24} + k5_{25} + k5_{26} + k5_{41} + k5_{43} + k5_{44} + k5_{45} + k5_{46} + k5_{47} + k5_{48}$$

$$0x72 = k3_{41} + k4_{14} + k4_{18} + k4_{31} + k4_{43} + k4_{47} + k5_{13} + k5_{17} + k5_{23} + k5_{27} + k5_{41} + k5_{44} + k5_{48}$$

$$0xa2 = k3_{42} + k4_{11} + k4_{15} + k4_{32} + k4_{41} + k4_{44} + k4_{45} + k4_{48} + k5_{11} + k5_{14} + k5_{15} + k5_{18} + k5_{21} + k5_{24} + k5_{25} + k5_{28} + k5_{41} + k5_{42} + k5_{45}$$

$$0x68 = k3_{43} + k4_{12} + k4_{16} + k4_{33} + k4_{41} + k4_{42} + k4_{45} + k4_{46} + k5_{11} + k5_{12} + k5_{15} + k5_{16} + k5_{21} + k5_{22} + k5_{25} + k5_{26} + k5_{42} + k5_{43} + k5_{46}$$

$$0x56 = k3_{44} + k4_{13} + k4_{14} + k4_{17} + k4_{18} + k4_{34} + k4_{42} + k4_{46} + k5_{12} + k5_{16} + k5_{22} + k5_{26} + k5_{43} + k5_{47} + k5_{48}$$

$$0x80 = k3_{45} + k4_{12} + k4_{13} + k4_{16} + k4_{18} + k4_{35} + k4_{42} + k4_{43} + k4_{47} + k5_{12} + k5_{13} + k5_{17} + k5_{22} + k5_{23} + k5_{27} + k5_{42} + k5_{43} + k5_{45} + k5_{46} + k5_{48}$$

$$0xda = k3_{46} + k4_{11} + k4_{13} + k4_{14} + k4_{15} + k4_{17} + k4_{36} + k4_{41} + k4_{43} + k4_{44} + k4_{45} + k4_{48} + k5_{11} + k5_{13} + k5_{14} + k5_{15} + k5_{18} + k5_{21} + k5_{23} + k5_{24} + k5_{25} + k5_{28} + k5_{41} + k5_{43} + k5_{44} + k5_{45} + k5_{46} + k5_{47}$$

$$0xc7 = k3_{47} + k4_{12} + k4_{14} + k4_{15} + k4_{16} + k4_{18} + k4_{37} + k4_{42} + k4_{44} + k4_{45} + k4_{46} + k5_{12} + k5_{14} + k5_{15} + k5_{16} + k5_{22} + k5_{24} + k5_{25} + k5_{26} + k5_{42} +$$

$k5_{44} + k5_{45} + k5_{46} + k5_{47} + k5_{48}$

$0x2c = k3_{48} + k4_{11} + k4_{12} + k4_{15} + k4_{17} + k4_{18} + k4_{38} + k4_{41} + k4_{42} + k4_{46} + k5_{11} + k5_{12} + k5_{16} + k5_{21} + k5_{22} + k5_{26} + k5_{41} + k5_{42} + k5_{45} + k5_{47}$

$0x5e = k4_{11} + k4_{13} + k4_{14} + k4_{15} + k4_{16} + k4_{17} + k4_{18} + k4_{41} + k4_{44} + k4_{46} + k4_{48} + k5_{14} + k5_{16} + k5_{18} + k5_{21} + k5_{24} + k5_{26} + k5_{28} + k5_{41} + k5_{43} + k5_{44} + k5_{45} + k5_{46} + k5_{47} + k5_{48} + k6_{11} + k6_{31}$

$0x69 = k4_{12} + k4_{14} + k4_{16} + k4_{17} + k4_{18} + k4_{41} + k4_{42} + k4_{45} + k4_{47} + k5_{11} + k5_{15} + k5_{17} + k5_{21} + k5_{22} + k5_{25} + k5_{27} + k5_{42} + k5_{44} + k5_{46} + k5_{47} + k5_{48} + k6_{12} + k6_{32}$

$0x66 = k4_{13} + k4_{14} + k4_{15} + k4_{18} + k4_{41} + k4_{42} + k4_{43} + k4_{48} + k5_{11} + k5_{13} + k5_{14} + k5_{18} + k5_{21} + k5_{22} + k5_{23} + k5_{28} + k5_{43} + k5_{44} + k5_{45} + k5_{48} + k6_{12} + k6_{14} + k6_{32} + k6_{34}$

$0x94 = k4_{14} + k4_{15} + k4_{16} + k4_{41} + k4_{42} + k4_{43} + k4_{44} + k4_{45} + k5_{12} + k5_{14} + k5_{15} + k5_{21} + k5_{22} + k5_{23} + k5_{24} + k5_{25} + k5_{44} + k5_{45} + k5_{46} + k6_{11} + k6_{13} + k6_{31} + k6_{33}$

$0x8f = k4_{15} + k4_{16} + k4_{41} + k4_{42} + k4_{43} + k4_{44} + k5_{15} + k5_{21} + k5_{22} + k5_{23} + k5_{24} + k5_{45} + k5_{46} + k6_{11} + k6_{12} + k6_{13} + k6_{14} + k6_{15} + k6_{31} + k6_{32} + k6_{33} + k6_{34} + k6_{35}$

$0x1b = k4_{16} + k4_{17} + k4_{42} + k4_{43} + k4_{44} + k5_{16} + k5_{22} + k5_{23} + k5_{24} + k5_{46} + k5_{47} + k6_{12} + k6_{13} + k6_{14} + k6_{16} + k6_{32} + k6_{33} + k6_{34} + k6_{36}$

$0x48 = k4_{17} + k4_{18} + k4_{42} + k4_{43} + k5_{15} + k5_{16} + k5_{18} + k5_{22} + k5_{23} + k5_{47} + k5_{48} + k6_{12} + k6_{13} + k6_{15} + k6_{16} + k6_{18} + k6_{32} + k6_{33} + k6_{35} + k6_{36} + k6_{38}$

$0x28 = k4_{18} + k4_{41} + k4_{43} + k4_{44} + k5_{15} + k5_{16} + k5_{17} + k5_{21} + k5_{23} + k5_{24} + k5_{48} + k6_{11} + k6_{13} + k6_{14} + k6_{15} + k6_{16} + k6_{17} + k6_{31} + k6_{33} + k6_{34} + k6_{35} + k6_{36} + k6_{37}$

$0x00 = k4_{21} + k4_{31} + k4_{45} + k5_{25} + k6_{15} + k6_{35}$

$0x00 = k4_{22} + k4_{32} + k4_{46} + k5_{26} + k6_{16} + k6_{36}$

$0x00 = k4_{23} + k4_{33} + k4_{47} + k5_{27} + k6_{17} + k6_{37}$

$0x00 = k4_{24} + k4_{34} + k4_{48} + k5_{28} + k6_{18} + k6_{38}$

$0x00 = k4_{25} + k4_{35} + k4_{41} + k5_{21} + k6_{11} + k6_{31}$

$0x00 = k4_{26} + k4_{36} + k4_{42} + k5_{22} + k6_{12} + k6_{32}$

$0x00 = k4_{27} + k4_{37} + k4_{43} + k5_{23} + k6_{13} + k6_{33}$

$0x00 = k4_{28} + k4_{38} + k4_{44} + k5_{24} + k6_{14} + k6_{34}$

$0x7b = k4_{41} + k4_{43} + k5_{16} + k5_{17} + k5_{18} + k5_{21} + k5_{23} + k5_{45} + k6_{11} + k6_{13} + k6_{16} + k6_{17} + k6_{18} + k6_{31} + k6_{33} + k6_{36} + k6_{37} + k6_{38} + k6_{45}$

$0x1b = k4_{42} + k4_{43} + k4_{44} + k5_{16} + k5_{22} + k5_{23} + k5_{24} + k5_{45} + k5_{46} + k6_{12} + k6_{13} + k6_{14} + k6_{16} + k6_{32} + k6_{33} + k6_{34} + k6_{36} + k6_{45} + k6_{46}$

$0xbc = k4_{43} + k4_{44} + k5_{17} + k5_{23} + k5_{24} + k5_{46} + k5_{47} + k6_{13} + k6_{14} + k6_{17} + k6_{33} + k6_{34} + k6_{37} + k6_{46} + k6_{47}$

$$0x53 = k4_{44} + k5_{15} + k5_{18} + k5_{24} + k5_{45} + k5_{47} + k5_{48} + k6_{14} + k6_{15} + k6_{18} + k6_{34} + k6_{35} + k6_{38} + k6_{45} + k6_{47} + k6_{48}$$

$$0x79 = k4_{45} + k4_{46} + k4_{47} + k5_{13} + k5_{25} + k5_{26} + k5_{27} + k5_{41} + k6_{13} + k6_{15} + k6_{16} + k6_{17} + k6_{33} + k6_{35} + k6_{36} + k6_{37} + k6_{41}$$

$$0xd8 = k4_{46} + k4_{47} + k4_{48} + k5_{11} + k5_{12} + k5_{26} + k5_{27} + k5_{28} + k5_{43} + k6_{11} + k6_{12} + k6_{16} + k6_{17} + k6_{18} + k6_{31} + k6_{32} + k6_{36} + k6_{37} + k6_{38} + k6_{43}$$

$$0xfb = k4_{47} + k4_{48} + k5_{12} + k5_{13} + k5_{27} + k5_{28} + k5_{41} + k5_{44} + k6_{12} + k6_{13} + k6_{17} + k6_{18} + k6_{32} + k6_{33} + k6_{37} + k6_{38} + k6_{41} + k6_{44}$$

$$0xba = k4_{48} + k5_{11} + k5_{13} + k5_{14} + k5_{28} + k5_{41} + k5_{42} + k6_{11} + k6_{13} + k6_{14} + k6_{18} + k6_{31} + k6_{33} + k6_{34} + k6_{38} + k6_{41} + k6_{42}$$

$$0x04 = k5_{11} + k5_{14} + k5_{15} + k5_{44} + k5_{45} + k5_{48} + k6_{11} + k6_{14} + k6_{15} + k6_{31} + k6_{34} + k6_{35} + k6_{43} + k6_{44} + k6_{45} + k6_{48} + k7_{13} + k7_{23}$$

$$0x25 = k5_{12} + k5_{17} + k5_{18} + k5_{42} + k5_{43} + k5_{44} + k5_{46} + k6_{12} + k6_{17} + k6_{18} + k6_{32} + k6_{37} + k6_{38} + k6_{41} + k6_{42} + k6_{43} + k6_{44} + k6_{46} + k7_{11} + k7_{21}$$

$$0x96 = k5_{13} + k5_{18} + k5_{43} + k5_{44} + k5_{47} + k6_{13} + k6_{18} + k6_{33} + k6_{38} + k6_{42} + k6_{43} + k6_{44} + k6_{47} + k7_{12} + k7_{22}$$

$$0xca = k5_{14} + k5_{15} + k5_{16} + k5_{17} + k5_{18} + k5_{41} + k5_{42} + k5_{43} + k5_{48} + k6_{14} + k6_{15} + k6_{16} + k6_{17} + k6_{18} + k6_{34} + k6_{35} + k6_{36} + k6_{37} + k6_{38} + k6_{41} + k6_{42} + k6_{44} + k6_{48} + k7_{13} + k7_{14} + k7_{23} + k7_{24}$$

$$0x94 = k5_{15} + k5_{16} + k5_{17} + k5_{18} + k5_{41} + k5_{44} + k5_{48} + k6_{15} + k6_{16} + k6_{17} + k6_{18} + k6_{35} + k6_{36} + k6_{37} + k6_{38} + k6_{41} + k6_{43} + k6_{48} + k7_{13} + k7_{14} + k7_{21} + k7_{23} + k7_{24} + k7_{31}$$

$$0xa7 = k5_{16} + k5_{17} + k5_{18} + k5_{41} + k5_{42} + k5_{45} + k6_{16} + k6_{17} + k6_{18} + k6_{36} + k6_{37} + k6_{38} + k6_{41} + k6_{42} + k6_{44} + k6_{45} + k7_{14} + k7_{22} + k7_{24} + k7_{32}$$

$$0xef = k5_{17} + k5_{18} + k5_{42} + k5_{43} + k5_{46} + k6_{17} + k6_{18} + k6_{37} + k6_{38} + k6_{41} + k6_{42} + k6_{43} + k6_{46} + k7_{11} + k7_{21} + k7_{23} + k7_{33}$$

$$0xc7 = k5_{18} + k5_{41} + k5_{43} + k5_{44} + k5_{47} + k6_{18} + k6_{38} + k6_{41} + k6_{42} + k6_{43} + k6_{44} + k6_{47} + k7_{12} + k7_{21} + k7_{22} + k7_{24} + k7_{31} + k7_{34}$$

$$0x69 = k5_{21} + k5_{31} + k5_{41} + k5_{43} + k5_{44} + k6_{41} + k6_{43} + k6_{44} + k7_{22} + k7_{32}$$

$$0xca = k5_{22} + k5_{32} + k5_{42} + k5_{44} + k6_{42} + k6_{44} + k7_{23} + k7_{33}$$

$$0x51 = k5_{23} + k5_{33} + k5_{41} + k5_{43} + k6_{41} + k6_{43} + k7_{21} + k7_{24} + k7_{31} + k7_{34}$$

$$0x5e = k5_{24} + k5_{34} + k5_{42} + k5_{43} + k6_{42} + k6_{43} + k7_{21} + k7_{31}$$

$$0x33 = k5_{25} + k5_{35} + k5_{42} + k5_{44} + k5_{48} + k6_{42} + k6_{43} + k6_{44} + k6_{48} + k7_{13} + k7_{21} + k7_{22} + k7_{23} + k7_{31} + k7_{32}$$

$$0x48 = k5_{26} + k5_{36} + k5_{41} + k5_{43} + k5_{45} + k6_{43} + k6_{44} + k6_{45} + k7_{11} + k7_{14} + k7_{21} + k7_{22} + k7_{23} + k7_{24} + k7_{32} + k7_{33}$$

$$0x28 = k5_{27} + k5_{37} + k5_{41} + k5_{42} + k5_{44} + k5_{46} + k6_{44} + k6_{46} + k7_{11} + k7_{12} + k7_{22} + k7_{23} + k7_{24} + k7_{31} + k7_{33} + k7_{34}$$

$$0xc7 = k5_{28} + k5_{38} + k5_{41} + k5_{43} + k5_{44} + k5_{47} + k5_{48} + k6_{41} + k6_{42} +$$

$k6_{43} + k6_{44} + k6_{47} + k6_{48} + k7_{12} + k7_{21} + k7_{22} + k7_{24} + k7_{31} + k7_{34}$

$0x09 = k5_{41} + k5_{42} + k5_{43} + k5_{44} + k6_{11} + k6_{41} + k6_{42} + k7_{13} + k7_{14} + k7_{21} + k7_{22} + k7_{23} + k7_{24} + k7_{31} + k7_{32} + k7_{41}$

$0x16 = k5_{42} + k5_{43} + k5_{44} + k6_{12} + k6_{42} + k6_{43} + k7_{14} + k7_{22} + k7_{23} + k7_{24} + k7_{32} + k7_{33} + k7_{42}$

$0xde = k5_{43} + k5_{44} + k6_{13} + k6_{41} + k6_{43} + k6_{44} + k7_{11} + k7_{23} + k7_{24} + k7_{31} + k7_{33} + k7_{34} + k7_{43}$

$0x2c = k5_{44} + k6_{11} + k6_{14} + k6_{42} + k6_{44} + k7_{12} + k7_{24} + k7_{32} + k7_{34} + k7_{41} + k7_{44}$

$0x02 = k5_{45} + k5_{47} + k6_{12} + k6_{13} + k6_{14} + k6_{16} + k6_{42} + k6_{43} + k6_{44} + k6_{45} + k6_{47} + k7_{12} + k7_{13} + k7_{14} + k7_{22} + k7_{23} + k7_{34} + k7_{42} + k7_{43} + k7_{44} + k7_{46}$

$0x43 = k5_{46} + k5_{48} + k6_{11} + k6_{12} + k6_{13} + k6_{14} + k6_{15} + k6_{41} + k6_{42} + k6_{43} + k6_{44} + k6_{46} + k6_{48} + k7_{11} + k7_{12} + k7_{13} + k7_{14} + k7_{21} + k7_{22} + k7_{33} + k7_{34} + k7_{41} + k7_{42} + k7_{43} + k7_{44} + k7_{45}$

$0x7d = k5_{47} + k6_{11} + k6_{13} + k6_{14} + k6_{15} + k6_{16} + k6_{17} + k6_{41} + k6_{43} + k6_{44} + k6_{47} + k7_{11} + k7_{13} + k7_{14} + k7_{24} + k7_{31} + k7_{33} + k7_{41} + k7_{43} + k7_{44} + k7_{45} + k7_{46} + k7_{47}$

$0x57 = k5_{48} + k6_{11} + k6_{14} + k6_{16} + k6_{18} + k6_{41} + k6_{44} + k6_{48} + k7_{11} + k7_{14} + k7_{21} + k7_{22} + k7_{23} + k7_{24} + k7_{32} + k7_{33} + k7_{41} + k7_{44} + k7_{46} + k7_{48}$

$0x37 = k6_{11} + k6_{14} + k6_{22} + k6_{32} + k6_{42} + k7_{12} + k7_{21} + k7_{22} + k7_{31} + k7_{41} + k7_{44}$

$0x94 = k6_{12} + k6_{14} + k6_{22} + k6_{23} + k6_{32} + k6_{33} + k6_{42} + k6_{43} + k7_{12} + k7_{13} + k7_{21} + k7_{23} + k7_{31} + k7_{32} + k7_{42} + k7_{44}$

$0x51 = k6_{13} + k6_{21} + k6_{31} + k6_{41} + k7_{11} + k7_{21} + k7_{24} + k7_{34} + k7_{43}$

$0x5e = k6_{14} + k6_{22} + k6_{23} + k6_{24} + k6_{32} + k6_{33} + k6_{34} + k6_{42} + k6_{43} + k6_{44} + k7_{12} + k7_{13} + k7_{14} + k7_{21} + k7_{31} + k7_{32} + k7_{33} + k7_{34} + k7_{44}$

$0x33 = k6_{15} + k6_{16} + k6_{17} + k6_{18} + k6_{22} + k6_{24} + k6_{25} + k6_{32} + k6_{34} + k6_{35} + k6_{41} + k7_{11} + k7_{21} + k7_{45} + k7_{46} + k7_{47} + k7_{48}$

$0x48 = k6_{16} + k6_{17} + k6_{18} + k6_{21} + k6_{23} + k6_{26} + k6_{31} + k6_{33} + k6_{36} + k6_{42} + k7_{12} + k7_{22} + k7_{46} + k7_{47} + k7_{48}$

$0x28 = k6_{17} + k6_{18} + k6_{21} + k6_{22} + k6_{24} + k6_{27} + k6_{31} + k6_{32} + k6_{34} + k6_{37} + k6_{43} + k7_{13} + k7_{23} + k7_{47} + k7_{48}$

$0xf4 = k6_{18} + k6_{21} + k6_{22} + k6_{23} + k6_{25} + k6_{28} + k6_{31} + k6_{32} + k6_{33} + k6_{35} + k6_{38} + k6_{41} + k6_{44} + k7_{11} + k7_{14} + k7_{21} + k7_{24} + k7_{48}$

$0xf7 = k6_{21} + k6_{25} + k6_{31} + k6_{35} + k6_{41} + k7_{11} + k7_{22} + k7_{24} + k7_{31} + k7_{32} + k7_{34} + k7_{43} + k8_{13} + k8_{23}$

$0xcc = k6_{22} + k6_{23} + k6_{24} + k6_{26} + k6_{27} + k6_{28} + k6_{32} + k6_{33} + k6_{34} + k6_{36} + k6_{37} + k6_{38} + k6_{42} + k6_{43} + k6_{44} + k7_{12} + k7_{13} + k7_{14} + k7_{21} + k7_{22} + k7_{31} + k7_{33} + k7_{34} + k7_{44} + k8_{14} + k8_{24}$

$0x52 = k6_{23} + k6_{24} + k6_{27} + k6_{28} + k6_{33} + k6_{34} + k6_{37} + k6_{38} + k6_{43} + k6_{44} + k7_{13} + k7_{14} + k7_{22} + k7_{23} + k7_{32} + k7_{34} + k7_{41} + k8_{11} + k8_{21}$

$0xf8 = k6_{24} + k6_{28} + k6_{34} + k6_{38} + k6_{44} + k7_{14} + k7_{21} + k7_{23} + k7_{24} + k7_{31} + k7_{33} + k7_{42} + k8_{12} + k8_{22}$

$0xf9 = k6_{25} + k6_{27} + k6_{28} + k6_{35} + k6_{37} + k6_{38} + k6_{41} + k6_{42} + k6_{44} + k7_{11} + k7_{12} + k7_{14} + k7_{22} + k7_{23} + k7_{24} + k7_{31} + k7_{33} + k7_{41} + k7_{42} + k7_{43} + k7_{44} + k7_{46} + k8_{11} + k8_{12} + k8_{13} + k8_{14} + k8_{16} + k8_{21} + k8_{22} + k8_{23} + k8_{24} + k8_{26}$

$0x60 = k6_{26} + k6_{27} + k6_{36} + k6_{37} + k6_{41} + k6_{43} + k7_{11} + k7_{13} + k7_{21} + k7_{22} + k7_{23} + k7_{24} + k7_{32} + k7_{34} + k7_{41} + k7_{42} + k7_{43} + k7_{45} + k8_{11} + k8_{12} + k8_{13} + k8_{15} + k8_{21} + k8_{22} + k8_{23} + k8_{25}$

$0xc1 = k6_{27} + k6_{28} + k6_{37} + k6_{38} + k6_{42} + k7_{12} + k7_{21} + k7_{22} + k7_{31} + k7_{41} + k7_{44} + k7_{45} + k7_{47} + k8_{11} + k8_{14} + k8_{15} + k8_{17} + k8_{21} + k8_{24} + k8_{25} + k8_{27}$

$0xc0 = k6_{28} + k6_{38} + k6_{43} + k7_{13} + k7_{22} + k7_{23} + k7_{32} + k7_{41} + k7_{42} + k7_{45} + k7_{46} + k7_{48} + k8_{11} + k8_{12} + k8_{15} + k8_{16} + k8_{18} + k8_{21} + k8_{22} + k8_{25} + k8_{26} + k8_{28}$

$0x2c = k6_{41} + k6_{43} + k7_{11} + k7_{13} + k7_{21} + k7_{22} + k7_{24} + k7_{32} + k7_{33} + k7_{34} + k7_{41} + k7_{43} + k7_{44} + k7_{45} + k8_{11} + k8_{13} + k8_{14} + k8_{15} + k8_{23} + k8_{24} + k8_{25} + k8_{31}$

$0xf5 = k6_{42} + k6_{43} + k6_{44} + k7_{12} + k7_{13} + k7_{14} + k7_{23} + k7_{24} + k7_{32} + k7_{41} + k7_{42} + k7_{43} + k7_{45} + k7_{46} + k8_{11} + k8_{12} + k8_{13} + k8_{15} + k8_{16} + k8_{23} + k8_{25} + k8_{26} + k8_{31} + k8_{32}$

$0x08 = k6_{43} + k6_{44} + k7_{13} + k7_{14} + k7_{24} + k7_{33} + k7_{41} + k7_{42} + k7_{43} + k7_{44} + k7_{46} + k7_{47} + k8_{11} + k8_{12} + k8_{13} + k8_{14} + k8_{16} + k8_{17} + k8_{21} + k8_{24} + k8_{26} + k8_{27} + k8_{32} + k8_{33}$

$0xc9 = k6_{44} + k7_{14} + k7_{21} + k7_{31} + k7_{34} + k7_{42} + k7_{43} + k7_{44} + k7_{45} + k7_{47} + k7_{48} + k8_{12} + k8_{13} + k8_{14} + k8_{15} + k8_{17} + k8_{18} + k8_{21} + k8_{22} + k8_{25} + k8_{27} + k8_{28} + k8_{31} + k8_{33} + k8_{34}$

$0xcd = k6_{45} + k7_{15} + k7_{21} + k7_{22} + k7_{23} + k7_{24} + k7_{25} + k7_{31} + k7_{32} + k7_{33} + k7_{34} + k7_{41} + k7_{46} + k7_{48} + k8_{11} + k8_{16} + k8_{18} + k8_{22} + k8_{23} + k8_{26} + k8_{28} + k8_{31} + k8_{32} + k8_{33}$

$0xfd = k6_{46} + k7_{16} + k7_{22} + k7_{23} + k7_{24} + k7_{26} + k7_{32} + k7_{33} + k7_{34} + k7_{42} + k7_{45} + k7_{47} + k8_{12} + k8_{15} + k8_{17} + k8_{21} + k8_{23} + k8_{24} + k8_{25} + k8_{27} + k8_{31} + k8_{32} + k8_{33} + k8_{34}$

$0xe1 = k6_{47} + k7_{17} + k7_{23} + k7_{24} + k7_{27} + k7_{33} + k7_{34} + k7_{43} + k7_{45} + k7_{46} + k7_{48} + k8_{13} + k8_{15} + k8_{16} + k8_{18} + k8_{22} + k8_{24} + k8_{25} + k8_{26} + k8_{28} + k8_{32} + k8_{33} + k8_{34}$

$0xe9 = k6_{48} + k7_{18} + k7_{21} + k7_{22} + k7_{23} + k7_{28} + k7_{31} + k7_{32} + k7_{33} + k7_{44} + k7_{45} + k7_{47} + k7_{48} + k8_{14} + k8_{15} + k8_{17} + k8_{18} + k8_{21} + k8_{22} + k8_{25} + k8_{27} + k8_{28} + k8_{31} + k8_{32} + k8_{34}$

$0x0a = k7_{11} + k7_{23} + k7_{24} + k7_{33} + k7_{34} + k7_{43} + k7_{44} + k8_{13} + k8_{14} + k8_{22} + k8_{32} + k8_{33} + k8_{34} + k8_{41}$

$$0x0d = k7_{12} + k7_{24} + k7_{34} + k7_{44} + k8_{14} + k8_{23} + k8_{33} + k8_{34} + k8_{42}$$

$$0xc0 = k7_{13} + k7_{21} + k7_{31} + k7_{41} + k8_{11} + k8_{21} + k8_{24} + k8_{34} + k8_{43}$$

$$0xa4 = k7_{14} + k7_{22} + k7_{23} + k7_{24} + k7_{32} + k7_{33} + k7_{34} + k7_{42} + k7_{43} + k7_{44} + k8_{12} + k8_{13} + k8_{14} + k8_{21} + k8_{31} + k8_{32} + k8_{33} + k8_{34} + k8_{44}$$

$$0x8c = k7_{15} + k7_{21} + k7_{22} + k7_{31} + k7_{32} + k7_{42} + k7_{43} + k7_{44} + k7_{45} + k8_{12} + k8_{13} + k8_{14} + k8_{15} + k8_{21} + k8_{23} + k8_{24} + k8_{25} + k8_{31} + k8_{32} + k8_{45}$$

$$0xdb = k7_{16} + k7_{22} + k7_{23} + k7_{32} + k7_{33} + k7_{43} + k7_{44} + k7_{46} + k8_{13} + k8_{14} + k8_{16} + k8_{22} + k8_{24} + k8_{26} + k8_{32} + k8_{33} + k8_{46}$$

$$0x58 = k7_{17} + k7_{21} + k7_{23} + k7_{24} + k7_{31} + k7_{33} + k7_{34} + k7_{44} + k7_{47} + k8_{14} + k8_{17} + k8_{21} + k8_{23} + k8_{27} + k8_{31} + k8_{33} + k8_{34} + k8_{47}$$

$$0x2e = k7_{18} + k7_{21} + k7_{24} + k7_{31} + k7_{34} + k7_{41} + k7_{42} + k7_{43} + k7_{44} + k7_{48} + k8_{11} + k8_{12} + k8_{13} + k8_{14} + k8_{18} + k8_{22} + k8_{23} + k8_{28} + k8_{31} + k8_{34} + k8_{48}$$

$$0x91 = k7_{21} + k7_{24} + k7_{31} + k7_{34} + k7_{41} + k7_{42} + k7_{43} + k7_{44} + k8_{11} + k8_{12} + k8_{13} + k8_{14} + k8_{23} + k8_{24} + k8_{26} + k8_{31} + k8_{32} + k8_{36}$$

$$0x68 = k7_{22} + k7_{24} + k7_{32} + k7_{34} + k7_{41} + k8_{11} + k8_{23} + k8_{26} + k8_{27} + k8_{31} + k8_{33} + k8_{36} + k8_{37}$$

$$0x1f = k7_{23} + k7_{33} + k7_{41} + k7_{42} + k7_{43} + k8_{11} + k8_{12} + k8_{13} + k8_{22} + k8_{23} + k8_{24} + k8_{25} + k8_{31} + k8_{34} + k8_{35}$$

$$0xbb = k7_{24} + k7_{34} + k7_{42} + k7_{44} + k8_{12} + k8_{14} + k8_{21} + k8_{22} + k8_{24} + k8_{26} + k8_{27} + k8_{28} + k8_{31} + k8_{36} + k8_{37} + k8_{38}$$

$$0xe6 = k7_{25} + k7_{35} + k7_{45} + k7_{46} + k7_{47} + k7_{48} + k8_{15} + k8_{16} + k8_{17} + k8_{18} + k8_{22} + k8_{23} + k8_{25} + k8_{27} + k8_{32} + k8_{33} + k8_{36} + k8_{38}$$

$$0x5d = k7_{26} + k7_{36} + k7_{46} + k7_{47} + k7_{48} + k8_{16} + k8_{17} + k8_{18} + k8_{21} + k8_{23} + k8_{24} + k8_{25} + k8_{26} + k8_{28} + k8_{31} + k8_{33} + k8_{34} + k8_{35} + k8_{37}$$

$$0x77 = k7_{27} + k7_{37} + k7_{47} + k7_{48} + k8_{17} + k8_{18} + k8_{22} + k8_{24} + k8_{25} + k8_{26} + k8_{27} + k8_{32} + k8_{34} + k8_{35} + k8_{36} + k8_{38}$$

$$0x42 = k7_{28} + k7_{38} + k7_{45} + k7_{46} + k7_{47} + k8_{15} + k8_{16} + k8_{17} + k8_{21} + k8_{22} + k8_{26} + k8_{28} + k8_{31} + k8_{32} + k8_{35} + k8_{37} + k8_{38}$$

$$0x78 = k7_{41} + k7_{45} + k7_{46} + k7_{48} + k8_{11} + k8_{15} + k8_{16} + k8_{18} + k8_{22} + k8_{24} + k8_{26} + k8_{31} + k8_{32} + k8_{34} + k8_{35} + k8_{38} + k8_{41} + k9_{11} + k9_{21}$$

$$0x85 = k7_{42} + k7_{45} + k7_{46} + k7_{47} + k8_{12} + k8_{15} + k8_{16} + k8_{17} + k8_{21} + k8_{23} + k8_{27} + k8_{31} + k8_{32} + k8_{33} + k8_{35} + k8_{36} + k8_{42} + k9_{12} + k9_{22}$$

$$0x16 = k7_{43} + k7_{45} + k7_{46} + k7_{47} + k7_{48} + k8_{13} + k8_{15} + k8_{16} + k8_{17} + k8_{18} + k8_{21} + k8_{22} + k8_{24} + k8_{25} + k8_{28} + k8_{31} + k8_{32} + k8_{33} + k8_{34} + k8_{36} + k8_{37} + k8_{43} + k9_{13} + k9_{23}$$

$$0x24 = k7_{44} + k7_{45} + k7_{47} + k8_{14} + k8_{15} + k8_{17} + k8_{21} + k8_{23} + k8_{24} + k8_{25} + k8_{31} + k8_{33} + k8_{37} + k8_{44} + k9_{14} + k9_{24}$$

$$0x7c = k7_{45} + k7_{47} + k7_{48} + k8_{15} + k8_{17} + k8_{18} + k8_{21} + k8_{22} + k8_{25} + k8_{26} + k8_{27} + k8_{28} + k8_{31} + k8_{32} + k8_{36} + k8_{43} + k8_{46} + k9_{13} + k9_{16} + k9_{23} + k9_{26}$$

$$0x42 = k7_{46} + k7_{47} + k8_{16} + k8_{17} + k8_{21} + k8_{24} + k8_{25} + k8_{26} + k8_{27} + k8_{31} + k8_{34} + k8_{35} + k8_{42} + k8_{45} + k9_{12} + k9_{15} + k9_{22} + k9_{25}$$

$$0x5d = k7_{47} + k7_{48} + k8_{17} + k8_{18} + k8_{21} + k8_{22} + k8_{23} + k8_{24} + k8_{25} + k8_{28} + k8_{31} + k8_{32} + k8_{33} + k8_{34} + k8_{35} + k8_{37} + k8_{41} + k8_{42} + k8_{44} + k8_{45} + k8_{47} + k9_{11} + k9_{12} + k9_{14} + k9_{15} + k9_{17} + k9_{21} + k9_{22} + k9_{24} + k9_{25} + k9_{27}$$

$$0x56 = k7_{48} + k8_{18} + k8_{22} + k8_{23} + k8_{24} + k8_{25} + k8_{26} + k8_{32} + k8_{33} + k8_{34} + k8_{35} + k8_{36} + k8_{38} + k8_{41} + k8_{42} + k8_{43} + k8_{45} + k8_{46} + k8_{48} + k9_{11} + k9_{12} + k9_{13} + k9_{15} + k9_{16} + k9_{18} + k9_{21} + k9_{22} + k9_{23} + k9_{25} + k9_{26} + k9_{28}$$

【０１２２】

ここで、下記式が成立する。

【０１２３】

【数４０】

$$\mathrm{rank}\,(M^{*}_{KH}) = N_m - N_r$$

【０１２４】

従って、上記１６８個の線形関係式は、互いに独立な線形関係式である。従って、これら１６８個のＧＦ（２）上の任意を線形結合して得られる$2^{168}-1$個の線形関係式が成り立つことがわかる。この線形関係式が多ければ、暗号の設計者の意図しない新たな攻撃を招く恐れがあるので、上述した方法によって得られた線形関係式の総数を、暗号強度評価の一つの指標として用いることができる。

【０１２５】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０１２６】

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【０１２７】

例えば、プログラムは記憶媒体としてのハードディスクやＲＯＭ（Read Only Memory)に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

【０１２８】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記憶媒体にインストールすることができる。

【０１２９】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。

【０１３０】

【発明の効果】

以上、説明したように、本発明の構成によれば、鍵スケジュールの複雑性に拘わらず、共通鍵ブロック暗号方式におけるラウンド鍵間の線形関係式をすべて網羅することが可能となり、導出される線形関係式に基づいて、共通鍵ブロック暗号方式の暗号強度評価を実行することが可能となる。

【０１３１】

本発明の構成によれば、暗号アルゴリズムのうち、鍵スケジュール部のアルゴリズムをベクトルと行列を用いて方程式で表現し、その行列方程式における非線形変換出力値及び初期値をユニタリ変換を利用して消去することにより、ラウン

ド鍵間の全ての線形関係式を求めることが可能となる。ラウンド鍵間に単純な依存関係が存在すると、実質的なラウンド鍵の数が減ってしまうことになるため、暗号の設計者は、このような関係式が多数存在することがないよう、注意する必要がある。本発明に係る方法によって、ラウンド鍵間の線形関係式の数が少なくなるよう、暗号鍵の強度を評価することによって、より安全な暗号を設計することが可能になる。

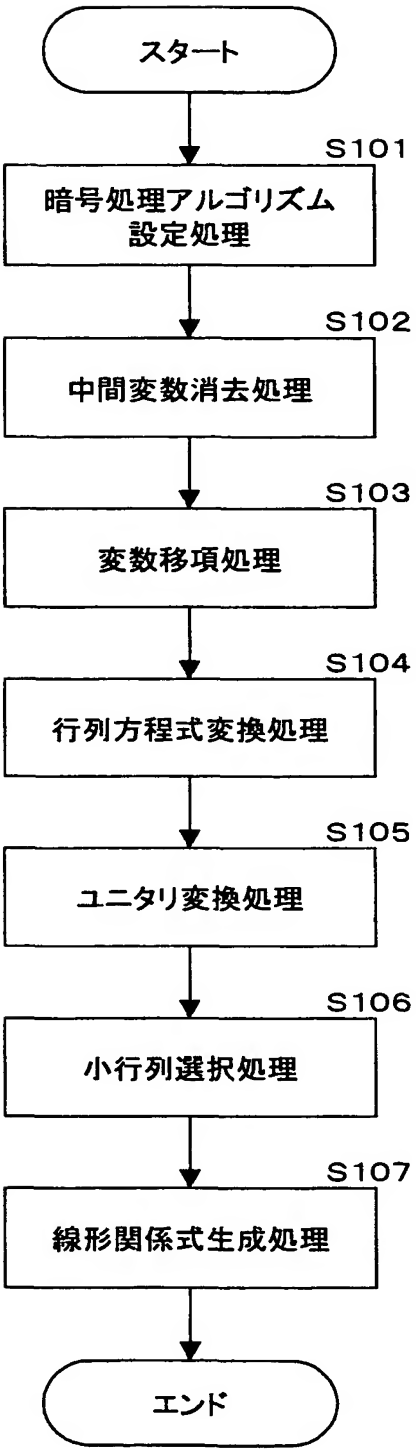
【図面の簡単な説明】

【図１】

本発明を適用した暗号強度指標算出処理手順を説明するフローチャートを示す図である。

【書類名】　　図面

【図１】


スタート
S101
暗号処理アルゴリズム
設定処理
S102
中間変数消去処理
S103
変数移項処理
S104
行列方程式変換処理
S105
ユニタリ変換処理
S106
小行列選択処理
S107
線形関係式生成処理
エンド

【書類名】　　要約書

【要約】

【課題】　共通鍵ブロック暗号における暗号強度評価処理を確実に実行する方法を提供する。

【解決手段】　共通鍵ブロック暗号アルゴリズムにおいて、鍵スケジュール部のアルゴリズムをベクトルと行列を用いて方程式で表現し、その行列方程式における非線形変換出力値及び初期値をユニタリ変換を利用して消去することにより、ラウンド鍵間の全ての線形関係式を求める。本方式によれば、鍵スケジュールの複雑性に拘わらず、共通鍵ブロック暗号方式におけるラウンド鍵間の線形関係式をすべて網羅することが可能となり、導出される線形関係式に基づいて、共通鍵ブロック暗号方式の暗号強度評価を実行することが可能となる。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
〔変更理由〕　新規登録
住　所　東京都品川区北品川６丁目７番３５号
氏　名　ソニー株式会社